Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to items appearing in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Bugs, Holes, & Patches

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Acute Websight Incorporated PeerFTP_5	A vulnerability exists in the 'Program Files\AcuteWebsight\PeerFTP_5\PeerFTP.ini' file, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. An exploit script has been published.	PeerFTP_5 FTP Password Disclosure CAN-2005-0517	Medium	SecurityTracker Alert, 1013263, February 23, 2005
ArGoSoft FTP Server 1.0, 1.2.2.2, 1.4.1 .1-1.4.1.9, 1.4.2.0-1.4.2.2, 1.4.2 .7	A vulnerability exists in the 'SITE COPY' command because shortcut files can be copied, which could let a malicious user obtain sensitive information. Upgrades available at: http://www.argosoft.com/dl/default.aspx?filename=fssetup.exe There is no exploit code required.	ArGoSoft FTP Server 'SITE COPY' Shortcut File CAN-2005-0520	Medium	Secunia Advisory, SA14372, February 23, 2005
Bfriendly.com Einstein 1.01 & prior	A vulnerability exists because usernames and passwords are stored in plaintext form in the Windows Registry, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. An exploit script has been published.	Einstein Password Disclosure	Medium	SecurityTracker Alert, 1013316, February 28, 2005
CIS WebServer 3.5.13	A Directory Traversal vulnerability exists when handling certain types of requests, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	CIS WebServer Remote Directory Traversal CAN-2005-0574	Medium	SecurityFocus, 12662, February 25, 2005
Computer Knacks, Inc. SendLink 1.5	A vulnerability exists in 'Program Files\SendLink\User\data.eat' because passwords are stored in plaintext, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. An exploit script has been published.	SendLink Password Disclosure CAN-2005-0521	Medium	SecurityTracker Alert, 1013269, February 23, 2005
eXeem eXeem 0.21	A vulnerability exists because plaintext passwords and configuration data is stored in the Windows Registry, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. An exploit script has been published.	eXeem Password Disclosure CAN-2005-0518	Medium	SecurityTracker Alert, 1013266, February 23, 2005
Gaim.sourceforge.net Gaim 1.1.3; possibly other versions	A remote Denial of Service vulnerability exists in the file transfer feature. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Gaim File Transfer Remote Denial of Service CAN-2005-0573	Low	SecurityTracker Alert, 1013300, February 28, 2005
GFI Ltd. LanGuard Network Security Scanner 5.0	A vulnerability exists in 'Inss.exe' because loaded saved credentials are stored in memory, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. An exploit script has been published.	GFI LANguard Network Security Scanner Password Disclosure CAN-2005-0604	Medium	Hat-Squad Advisory, February 28, 2005
KMiNT21 Software Golden FTP Server Pro 2.05b & prior	A buffer overflow vulnerability exists when a specially crafted RNTO command is submitted, which could let a remote malicious user execute arbitrary code.	Golden FTP Server RNTO Command Buffer Overflow	High	Secunia Advisory, SA13966, January 24, 2005

	Update available at: http://www.goldenftpserver.com/download.htm An exploit script has been published.	CAN-2005-0566		**US-CERT VU#620862**
LionMax Software ChatAnywhere 2.72a	A vulnerability exists in the 'Program Files\Chat Anywhere\room\[chatroomname].ini' file because passwords and usernames are stored in plaintext, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. An exploit script has been published.	Chat Anywhere Password Disclosure CAN-2005-0522	Medium	SecurityTracker Alert, 1013270, February 23, 2005
MercurySteam Entertainment Scrapland 1.0	Several remote Denial of Service vulnerabilities exist due to a failure to handle exceptional conditions. No workaround or patch available at time of publishing. An exploit script has been published.	MercurySteam Scrapland Game Server Remote Denials of Service	Low	Secunia Advisory, SA14435, March 1, 2005
Microsoft Office XP SP2 & SP3, Project 2002, Visio 2002, Works Suite 2002, 2003, 2004	A buffer overflow vulnerability exists due to a boundary error in the process that passes URL file locations to Office, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-005.mspx V1.1: Bulletin updated to clarify prerequisites under Visio 2002 Update Information. **V1.2: Bulletin updated to add an additional FAQ as well as clarify install steps under Update Information.** Currently we are not aware of any exploits for this vulnerability.	Microsoft Office URL File Location Handling Buffer Overflow CAN-2004-0848	High	Microsoft Security Bulletin, MS05-005, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT VU#416001 Microsoft Security Bulletin, MS05-005 V1.1, February 15, 2005 **Microsoft Security Bulletin, MS05-005 V1.2, February 23, 2005**
Microsoft Windows Server 2003 Datacenter Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Exchange Server 2003	A remote code execution vulnerability exists in the Windows Server 2003 SMTP component due to the way Domain Name System (DNS) lookups are handled. A malicious user could exploit the vulnerability by causing the server to process a particular DNS response that could potentially allow remote code execution. The vulnerability also exists in the Microsoft Exchange Server 2003 Routing Engine component when installed on Microsoft Windows 2000 Service Pack 3 or on Microsoft Windows 2000 Service Pack 4. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-035.mspx Bulletin updated to clarify restart requirement for Windows Server 2003 and Windows XP 64-Bit. Bulletin updated to advise of the availability of an update for Exchange 2000 Server. **V2.1: Bulletin updated to clarify restart requirement for Exchange 2000 Server** Currently we are not aware of any exploits for this vulnerability.	Microsoft SMTP Remote Code Execution CAN-2004-0840	High	Microsoft Security Bulletin, MS04-035, October 12, 2004 US-CERT Cyber Security Alert, SA04-286A US-CERT VU#394792 Microsoft Security Bulletin MS04-035, November 9, 2004 Microsoft Security Bulletin MS04-035 V2.0 February 8, 2005 **Microsoft Security Bulletin MS04-035 V2.1 February 23, 2005**
Microsoft Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1-SP4, 2000 Professional, SP1-SP4, 2000 Server, SP1-SP4	A vulnerability exists due to the way group policies are enforced, which could let a malicious user bypass drive access restriction. No workaround or patch available at time of publishing. There is no exploit code required.	Microsoft Windows 2000 Group Restriction Bypass CAN-2005-0545	Medium	SecurityFocus, 12641, February 23, 2005

Microsoft Windows NT Server 4.0 SP6a, Windows NT Server 4.0 Terminal Server Edition SP6a, Windows 2000 Server SP3 & SP4, Windows 2003, Windows 2003 for Itanium-based Systems	A buffer overflow vulnerability exists in the License Logging service due to a boundary error, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-010.mspx **V1.1: Bulletin updated to reflect a revised "Security Update Information" section for Windows Server 2003** Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows License Logging Service Buffer Overflow CAN-2005-0050	Low/High (High if arbitrary code can be executed)	Microsoft Security Bulletin, MS05-010, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT VU#130433 **Microsoft Security Bulletin, MS05-010 V1.1, February 23, 2005**
Multiple Vendors Mozilla Browser 1.7.5, Firefox 1.0, Netscape Netscape 7.1	A vulnerability exists because popup windows can overlay modal dialogs, which could lead to a false sense of security. **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** **Mozilla:** **http://ftp.mozilla.org/pub/mozilla.org/firefox/releases/1.0.1/source/firefox-1.0.1-source.tar.bz2** Proofs of Concept exploits have been published.	Mozilla/Netscape/Firefox Browser Modal Dialog Spoofing	Medium	Securiteam, January 11, 2005 **Fedora Update Notification, FEDORA-2005-182, February 26, 2005**
NullSoft Winamp 5.07	A remote Denial of Service vulnerability exists due to a failure to properly process '.mp4' and '.m4a' files. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Nullsoft Winamp Malformed MP4 Remote Denial of Service **CAN-2004-1119**	Low	SecurityTracker Alert ID, 1012525, December 15, 2004 **US-CERT VU#986504**
OpenConnect Systems WebConnect 6.4.4, 6.5	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists when a malicious user submits a request that has an MS-DOS device name; and a vulnerability exists in the "jretest.html' script due to insufficient validation of the 'WCP_USER' parameter, which could let a remote malicious user obtain sensitive information. Updates available at: http://www.oc.com/solutions/webconnect.jsp **Exploit scripts have been published.**	WebConnect Remote Denial of Service and Information Disclosure CAN-2004-0465 CAN-2004-0466	Low/Medium (Medium if sensitive information can be obtained)	CIRT Advisory, February 20, 2005 **PacketStorm, February 26, 2005** **US-CERT VU#628411** **US-CERT VU#552561**
RaidenHTTPD TEAM RaidenHTTPD 1.1.32	Several vulnerabilities exist: a vulnerability exists in the default installation CGI scripts, which could let a malicious user obtain sensitive information; and a buffer overflow vulnerability exists when processing long URI HTTP requests, which could let a malicious user execute arbitrary code. Upgrade available at: http://www.raidenhttpd.com/en/download.html Currently we are not aware of any exploits for these vulnerabilities.	RaidenHTTPD Multiple Remote Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	SIG^2 Vulnerability Research Advisory, March 1, 2005
Stormy Studios KNet 1.0, 1.2, 1.3, 1.4 c, 1.4 b	A buffer overflow vulnerability exists due to a failure to securely copy user-supplied input into finite process buffers, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Stormy Studios KNet Remote Buffer Overflow CAN-2005-0575	High	SecurityFocus, 12671, February 25, 2005
Working Resources Inc. BadBlue 2.55	A buffer overflow vulnerability exists in 'ext.dll' in the 'mfcisapicommand' parameter due to a boundary error when processing HTTP requests, which could let a remote malicious user execute arbitrary code. Upgrade available at: http://badblue.com/bb95.exe Exploit scripts have been published.	Working Resources BadBlue MFCISAPICommand Remote Buffer Overflow CAN-2005-0595	High	SIA International Security Advisory, February 26, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Carnegie Mellon University Cyrus IMAP Server 2.x	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in mailbox handling due to an off-by-one boundary error, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the imapd annotate extension due to an off-by-one boundary error, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in 'fetchnews,' which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exist because remote administrative users can exploit the backend; and a buffer overflow vulnerability exists in imapd due to a boundary error, which could let a remote malicious user execute arbitrary code. Update available at: http://ftp.andrew.cmu.edu/pub/cyrus/ cyrus-imapd-2.2.11.tar.gz Gentoo: http://security.gentoo.org/ glsa/glsa-200502-29.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/ pool/main/c/cyrus21-imapd/ Currently we are not aware of any exploits for these vulnerabilities.	Cyrus IMAP Server Multiple Remote Buffer Overflows CAN-2005-0546	High	Secunia Advisory, SA14383, February 24, 2005 Gentoo Linux Security Advisory, GLSA 200502-29, February 23, 2005 SUSE Security Announcement, SUSE-SA:2005:009, February 24, 2005 Ubuntu Security Notice USN-87-1, February 28, 2005
Carnegie Mellon University Cyrus SASL 1.5.24, 1.5.27, 1.5.28, 2.1.9-2.1.18	Several vulnerabilities exist: a buffer overflow vulnerability exists in 'digestmda5.c,' which could let a remote malicious user execute arbitrary code; and an input validation vulnerability exists in the 'SASL_PATH' environment variable, which could let a malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/ glsa/glsa-200410-05.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/ RHSA-2004-546.html Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/ main/c/cyrus-sasl/ Conectiva: ftp://atualizacoes.conectiva.com.br/ OpenPGK: ftp ftp.openpkg.org FedoraLegacy: http://download.fedoralegacy.org/redhat/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for these vulnerabilities.	Cyrus SASL Buffer Overflow & Input Validation CAN-2004-0884	High	SecurityTracker Alert ID: 1011568, October 7, 2004 Debian Security Advisories DSA 563-2, 563-3, & 568-1, October 12, 14, & 16, 2004 Conectiva Linux Security Announcement, CLA-2004:889, November 11, 2004 OpenPKG Security Advisory, OpenPKG Security Advisory, January 28, 2005 Fedora Legacy Update Advisory, FLSA:2137, February 17, 2005 **SUSE Security Summary Report, SUSE-SR:2005:006, February 25, 2005**
Daisuke NISHIKAWA DNA mkbold-mkitalic 0.1-0.6	A format string vulnerability exists when converting BDF font files, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://hp.vector.co.jp/authors/ VA013651/lib/mkbold-mkitalic-0.08.tar.bz2 Currently we are not aware of any exploits for this vulnerability.	DNA MKBold-MKItalic Remote Format String CAN-2005-0577	High	Secunia Advisory: SA14398, February 25, 2005
Debian reportbug 2.60, 2.6	Multiple vulnerabilities exist: a vulnerability exists in '.reportbugrc' files because it contains world-readable permissions, which could let a malicious user obtain sensitive information; and a vulnerability exists in 'smtppasswd' password setting because it is included in '.bugreportrc' which could let a malicious user obtain sensitive information. Ubuntu: http://security.ubuntu.com/ubuntu/	Debian Reportbug Multiple Information Disclosure	Medium	Ubuntu Security Notice USN-88-1 , February 28, 2005

	pool/main/r/reportbug/ There is no exploit code required.			
GNU Midnight Commander Project Midnight Commander 4.x	Multiple vulnerabilities exist due to various design and boundary condition errors, which could let a remote malicious user cause a Denial of Service, obtain elevated privileges, or execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/m/mc/ SUSE: ftp://ftp.suse.com/pub/suse/ Gentoo: http://security.gentoo.org/glsa/glsa-200502-24.xml **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for these vulnerabilities.	Midnight Commander Multiple Vulnerabilities CAN-2004-1004 CAN-2004-1005 CAN-2004-1009 CAN-2004-1090 CAN-2004-1091 CAN-2004-1092 CAN-2004-1093 CAN-2004-1174 CAN-2004-1175 CAN-2004-1176	Low/ Medium/ High (Low if a DoS; Medium is elevated privileges can be obtained; and High if arbitrary code can be executed)	SecurityTracker Alert, 1012903, January 14, 2005 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 Gentoo Linux Security Advisory, GLSA 200502-24, February 17, 2005 **Turbolinux Security Announcement, TLSA-24022005, February 24, 2005**
GNU Emacs prior to 21.4.17	A format string vulnerability exists in 'movemail.c,' which could let a remote malicious user execute arbitrary code. Update available at: ftp://ftp.xemacs.org/pub/xemacs/xemacs-21.4 Debian: http://security.debian.org/pool/.../e/emacs20/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/emacs21/ Gentoo: http://security.gentoo.org/glsa/glsa-200502-20.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Debian: http://security.debian.org/pool/updates/main/e/emacs21/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	Emacs Format String CAN-2005-0100	High	SecurityTracker Alert, 1013100, February 7, 2005 Debian Security Advisory, DSA-670-1 & 671-1, February 8, 2005 Ubuntu Security Notice, USN-76-1, February 7, 2005 Fedora Update Notifications FEDORA-2005-145 & 146, February 14, 2005 Gentoo Linux Security Advisory, GLSA 200502-20, February 15, 2005 Mandrakelinux Security Update Advisory,MDKSA-2005:03, February 15, 2005 Debian Security Advisory, DSA 685-1, February 17, 2005 **SUSE Security Summary Report, SUSE-SR:2005:006, February 25, 2005**

GNU Vim 6.x, GVim 6.x	Multiple vulnerabilities exist which can be exploited by local malicious users to gain escalated privileges. The vulnerabilities are caused due to some errors in the modelines options. This can be exploited to execute shell commands when a malicious file is opened. Successful exploitation can lead to escalated privileges but requires that modelines is enabled. Apply patch for vim 6.3: ftp://ftp.vim.org/pub/vim/patches/6.3/6.3.045 Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-10.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-010.html Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-020_RHSA-2005-019.pdf OpenPKG: ftp.openpkg.org Mandrake: http://www.mandrakesecure.net/en/ftp.php Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/v/vim/ SGI: http://support.sgi.com/ **Fedora: http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for these vulnerabilities.	GNU Vim / Gvim Modelines Command Execution Vulnerabilities CAN-2004-1138	Medium	Gentoo Linux Security Advisory, GLSA 200412-10 / vim, December 15, 2004 **Fedora Legacy Update Advisory, FLSA:2343, February 24, 2005**
GNU wget 1.9.1	A vulnerability exists which could permit a remote malicious user to create or overwrite files on the target user's system. wget does not properly validate user-supplied input. A remote user can bypass the filtering mechanism if DNS can be modified so that '..' resolves to an IP address. A specially crafted HTTP response can include control characters to overwrite portions of the terminal window. **SUSE: ftp://ftp.SUSE.com/pub/SUSE** A Proof of Concept exploit script has been published.	GNU wget File Creation & Overwrite CAN-2004-1487 CAN-2004-1488	Medium	SecurityTracker Alert ID: 1012472, December 10, 2004 SUSE Security Summary Report, SUSE-SR:2005:004, February 11, 2005 **SUSE Security Summary Report, SUSE-SR:2005:006, February 25, 2005**
GNU xine prior to 0.99.3	Multiple vulnerabilities exist that could allow a remote user to execute arbitrary code on the target user's system. There is a buffer overflow in pnm_get_chunk() in the processing of the RMF_TAG, DATA_TAG, PROP_TAG, MDPR_TAG, and CONT_TAG parameters. The vendor has issued a fixed version of xine-lib (1-rc8), available at: http://xinehq.de/index.php/releases A patch is also available at: http://cvs.sourceforge.net/viewcvs.py/xine/xine-lib/src/input/pnm.c?r1=1.20&r2=1.21 Conectiva: ftp://atualizacoes.conectiva.com.br/ Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200501-07.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.SUSE.com/pub/SUSE **TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** A Proof of Concept exploit has been published.	GNU xine Buffer Overflow in pnm_get_chunk() CAN-2004-1187 CAN-2004-1188	High	iDEFENSE Security Advisory 12.21.04 Gentoo, GLSA 200501-07, January 6, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:011, January 19, 2005 SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005 **Turbolinux Security Announcement, TLSA-24022005, February 24, 2005**

GNU xine-lib 1.x	Multiple vulnerabilities with unknown impacts exist due to errors in the PNM and Real RTSP clients. Update to version 1-rc8: http://xinehq.de/index.php/download Gentoo: http://security.gentoo.org/glsa/glsa-200501-07.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.SUSE.com/pub/SUSE **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for these vulnerabilities.	GNU xine-lib Unspecified PNM & Real RTSP Clients Vulnerabilities CAN-2004-1300	Not Specified	Secunia Advisory, SA13496, December 16, 2004 Gentoo Linux Security Advisory, GLSA 200501-07, January 6, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:011, January 19, 2005 SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005 **Turbolinux Security Announcement, TLSA-24022005, February 24, 2005**
Hewlett Packard Company HP-UX B.11.00, B.11.04, B.11.11, B.11.22, B.11.23	A vulnerability exists in ftpd which could let a remote malicious user obtain unauthorized access. Updates available at: http://software.hp.com/ Currently we are not aware of any exploits for this vulnerability.	HP-UX ftpd Remote Unauthorized Access CAN-2005-0547	Medium	HP Security Bulletin, HPSBUX01119, February 23, 2005
Hewlett Packard HP-UX 11.x	A vulnerability exists in HP-UX, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to a boundary error in the debug logging routine of ftpd. This can be exploited to cause a stack-based buffer overflow by sending a specially crafted, overly long command request. Successful exploitation may allow execution of arbitrary code, but requires that the FTP daemon is configured to log debug information (not default setting). Apply patches: http://www.itrc.hp.com/service/patch/mainPage.do HP: http://itrc.hp.com Currently we are not aware of any exploits for this vulnerability.	Hewlett Packard HP-UX FTP Server Debug Logging Buffer Overflow Vulnerability CAN-2004-1332	High	iDEFENSE Security Advisory 12.21.04 HP Security Bulletin, HPSBUX01118, February 9, 2005 **US-CERT VU#647438**
IBM AIX 5.2, 5.3	A format string vulnerability exists in auditselect, which could let a malicious user obtain root privileges. Updates available at: http://www-1.ibm.com/servers/eserver/support/pseries/aixfixes.html Currently we are not aware of any exploits for this vulnerability.	IBM AIX auditselect Format String CAN-2005-0250	High	SecurityTracker Alert, 1013103, February 8, 2005 **US-CERT VU#896729**
Jouni Malinen wpa_supplicant prior to 0.2.7 and 0.3.8	A remote Denial of Service vulnerability exists in 'wpa.c' when processing WPA2 frames due to insufficient validation of the Key Data Length. Update available at: http://hostap.epitest.fi/wpa_supplicant/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200502-22.xml** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	Jouni Malinen wpa_supplicant Remote Denial of Service CAN-2005-0470	Low	SecurityTracker Alert, 1013226, February 17, 2005 **Gentoo Linux Security Advisory, GLSA 200502-22, February 25, 2005** **SUSE Security Summary Report, SUSE-SR:2005:006, February 25, 2005**
Kalum Somaratna ProZilla Download Accelerator 1.0 x, 1.3.0-1.3.4, 1.3.5 .2, 1.3.5 .1, 1.3.5-1.3.5.2 1.3.6	A vulnerability exists due to improper implementation of a formatted string function when handling initial server responses, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. An exploit script has been published.	ProZilla Initial Server Response Format String CAN-2005-0523	High	SecurityFocus, 12635, February 23, 2005
Krzysztof Dabrowski cmd5checkpw 0.20-0.22	A vulnerability exists in the 'poppasswd' file, which could let a malicious user obtain sensitive information. Gentoo: http://security.gentoo.org/glsa/glsa-200502-30.xml There is no exploit code required.	Cmd5checkpw Poppasswd Disclosure CAN-2005-0580	Medium	Gentoo Linux Security Advisor, GLSA 200502-30, February 25, 2005

LGPL NASM 0.98.38	A vulnerability was reported in NASM. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted asm file that, when processed by the target user with NASM, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the error() function in 'preproc.c.' Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-20.xml Debian: http://www.debian.org/security/2005/dsa-623 Mandrake: http://www.mandrakesoft.com/security/advisories **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** A Proof of Concept exploit script has been published.	LGPL NASM error() Buffer Overflow CAN-2004-1287	High	Secunia Advisory ID, SA13523, December 17, 2004 Debian Security Advisory DSA-623-1 nasm, January 4, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:004, January 6, 2005 **Turbolinux Security Announcement, TLSA-24022005, February 24, 2005**
MIT Kerberos 5 krb5-1.3.5 & prior; Avaya S8700/S8500/S8300 (CM2.0 and later), MN100, Intuity LX 1.1- 5.x, Modular Messaging MSS	A buffer overflow exists in the libkadm5srv administration library. A remote malicious user may be able to execute arbitrary code on an affected Key Distribution Center (KDC) host. There is a heap overflow in the password history handling code. A patch is available at: http://web.mit.edu/kerberos/advisories/2004-004-patch_1.3.5.txt Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200501-05.xml Debian: http://security.debian.org/pool/updates/main/k/krb5/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/k/krb5/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-036_RHSA-2005-012.pdf **Sun:** **http://sunsolve.sun.com/search/document.do?assetkey=1-26-57712-1** Currently we are not aware of any exploits for this vulnerability.	Kerberos libkadm5srv Heap Overflow CAN-2004-1189	High	SecurityTracker Alert ID, 1012640, December 20, 2004 Gentoo GLSA 200501-05, January 5, 2005 Ubuntu Security Notice, USN-58-1, January 10, 2005 Conectiva Linux Security Announcement, CLA-2005:917, January 13, 2005 Avaya Security Advisory, ASA-2005-036, February 7, 2005 **Sun(sm) Alert Notification, 57712, February 25, 2005**
Mozilla.org Firefox 1.0	A vulnerability exists because a predictable name issued for the plugin temporary directory, which could let a malicious user cause a Denial of Service or modify system/user information. Update available at: http://www.mozilla.org/products/firefox/all.html An exploit has been published.	Mozilla Firefox Predictable Plugin Temporary Directory CAN-2005-0578	Low/Medium (Medium if user/system information can be modified)	Mozilla Foundation Security Advisory, 2005-28, February 25, 2005
Multiple Vendors Bernd Johanness Wueb kppp 1.1.3; KDE KDE 1.1-1.1.2, 1.2, 2.0 BETA, 2.0-2.2.2, 3.0-3.0.5, 3.1-3.1.5, KDE KPPP 2.1.2	A vulnerability exists due to a file descriptor leak, which could let a malicious user obtain sensitive information. Patch available at: ftp://ftp.kde.org/pub/kde/security_patches There is no exploit code required.	KPPP Privileged File Descriptor Information Disclosure CAN-2005-0205	Medium	iDEFENSE Security Advisory, February 28, 2005
Multiple Vendors FreeNX 0.2 -0-0.2 -3, 0.2.4-0.2.7	A vulnerability exists in the 'XAUTHORITY' environment variable, which could let a malicious user bypass authentication. Update available at: http://debian.tu-bs.de/knoppix/nx/freenx-0.2.8.tar.gz SuSE: ftp://ftp.suse.com/pub/suse/ There is no exploit code required.	FreeNX 'XAUTHORITY' Authentication Bypass CAN-2005-0579	Medium	SUSE Security Summary Report, ID: SUSE-SR:2005:006, February 25, 2005

Multiple Vendors Linux Kernel 2.4 - 2.4.28, 2.6 - 2.6.9; Avaya Converged Communications Server 2.0, Avaya Intuity LX, Avaya MN100, Avaya Modular Messaging (MSS) 1.1, 2.0, Avaya Network Routing Avaya S8300 R2.0.1, R2.0.0, S8500 R2.0.1, R2.0.0, S8700 R2.0.1, R2.0.0, S8710 R2.0.1, R2.0.0	A vulnerability was reported in the Linux kernel in the auxiliary message (scm) layer. A local malicious user can cause Denial of Service conditions. A local user can send a specially crafted auxiliary message to a socket to trigger a deadlock condition in the __scm_send() function. Ubuntu: http://security.ubuntu.com/ubuntu/pool/ SUSE: http://www.novell.com/linux/security/advisories/2004_44_kernel.html Trustix: http://http.trustix.org/pub/trustix/updates/ Red Hat: http://rhn.redhat.com/errata/RHSA-2004-689.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-006_RHSA-2004-549RHSA-2004-505RHSA-2004-689.pdf Mandrake: http://www.mandrakesecure.net/en/ftp.php **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/** A Proof of Concept exploit script has been published.	Multiple Vendors Linux Kernel Auxiliary Message Layer State Error CAN-2004-1016	Low	iSEC Security Research Advisory 0019, December 14, 2004 SecurityFocus, December 25, 2004 Secunia, SA13706, January 4, 2005 Avaya Security Advisory, ASA-2005-006, January 14, 2006 Mandrake Security Advisory, MDKSA-2005:022, January 26, 200 **Fedora Legacy Update Advisory, FLSA:2336, February 24, 2005** **Turbolinux Security Announcement , February 28, 2005**
Multiple Vendors Linux Kernel 2.4 - 2.4.28, 2.6 - 2.6.9; Avaya Intuity LX, Avaya MN100, Avaya Modular Messaging (MSS) 1.1, 2.0	Several vulnerabilities exist in the Linux kernel in the processing of IGMP messages. A local user may be able to gain elevated privileges. A remote user can cause the target system to crash. These are due to flaws in the ip_mc_source() and igmp_marksources() functions. SUSE: http://www.novell.com/linux/security/advisories/2004_44_kernel.html Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-006_RHSA-2004-549RHSA-2004-505RHSA-2004-689.pdf Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/** **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** A Proof of Concept exploit script has been published.	Multiple Vendors Linux Kernel IGMP Integer Underflow CAN-2004-1137	Low/ Medium (Medium if elevated privileges can be obtained)	iSEC Security Research Advisory 0018, December 14, 2004 SecurityFocus, December 25, 2005 Secunia, SA13706, January 4, 2005 Avaya Security Advisory, ASA-2005-006, January 14, 2006 Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 **Turbolinux Security Announcement , February 28, 2005** **Fedora Legacy Update Advisory, FLSA:2336, February 24, 2005**
Multiple Vendors Linux Kernel 2.4.x; Avaya Intuity LX, Avaya MN100, Avaya Modular Messaging (MSS)	Two vulnerabilities exist in the Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service) or potentially gain escalated privileges. 1) A boundary error exists in the system call handling in the 32bit system call emulation on AMD64 / Intel EM64T systems. 2) An unspecified error within the memory management handling of ELF executables in "load_elf_binary" can be exploited to crash the system via a specially crafted ELF binary (this issue only affects Kernel versions prior to	Multiple Vendors Linux Kernel 32bit System Call Emulation and ELF Binary Vulnerabilities	Medium	Secunia, SA SA13627, December 24, 2004 Red Hat RHSA-2004-689, December 23, 2004 Avaya Security Advisory,

1.1, 2.0, Network Routing	2.4.26). Issue 2 has been fixed in Kernel version 2.4.26 and later. Red Hat: http://rhn.redhat.com/errata/RHSA-2004-689.html Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-006_RHSA-2004-549RHSA-2004-505RHSA-2004-689.pdf **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for these vulnerabilities.	CAN-2004-1144 CAN-2004-1234		ASA-2005-006, January 14, 2006 **Fedora Legacy Update Advisory, FLSA:2336, February 24, 2005**
Multiple Vendors Linux Kernel 2.6.x	Some potential vulnerabilities exist with an unknown impact in the Linux Kernel. The vulnerabilities are caused due to boundary errors within the 'sys32_ni_syscall()' and 'sys32_vm86_warning()' functions and can be exploited to cause buffer overflows. Immediate consequences of exploitation of this vulnerability could be a kernel panic. It is not currently known whether this vulnerability may be leveraged to provide for execution of arbitrary code. Patches are available at: http://linux.bkbits.net:8080/linux-2.6/cset@1.2079 http://linux.bkbits.net:8080/linux-2.6/gnupatch@41ae6af1cR3mJYlW6D8EHxCKSxuJiQ Ubuntu: http://security.ubuntu.com/ubuntu/pool/ SUSE: http://www.novell.com/linux/security/advisories/2004_44_kernel.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendors Linux Kernel 'sys32_ni_syscall' and 'sys32_vm86_warning' Buffer Overflows CAN-2004-1151	Low/High (High if arbitrary code can be executed)	Secunia Advisory ID, SA13410, December 9, 2004 SecurityFocus, December 14, 2004 SecurityFocus, December 25, 2004 Secunia, SA13706, January 4, 2005 Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005 **Turbolinux Security Announcement , February 28, 2005**
Multiple Vendors Linux Kernel versions except 2.6.9	A race condition vulnerability exists in the Linux Kernel terminal subsystem. This issue is related to terminal locking and is exposed when a remote malicious user connects to the computer through a PPP dialup port. When the remote user issues the switch from console to PPP, there is a small window of opportunity to send data that will trigger the vulnerability. This may cause a Denial of Service. This issue has been addressed in version 2.6.9 of the Linux Kernel. Patches are also available for 2.4.x releases: http://www.kernel.org/pub/linux/kernel/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main Mandrake: http://www.mandrakesecure.net/en/ftp.php **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel Terminal Locking Race Condition CAN-2004-0814	Low	SecurityFocus, December 14, 2004 Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005 **Fedora Legacy Update Advisory, FLSA:2336, February 24, 2005** **Turbolinux Security Announcement , February 28, 2005**
Multiple Vendors bsmtpd bsmtpd 2.3; Debian Linux 3.0 sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	A vulnerability exists in the bsmtpd daemon due to insufficient sanitization of e-mail addresses, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/b/bsmtpd/ Currently we are not aware of any exploits for this vulnerability.	BSMTPD Remote Arbitrary Command Execution CAN-2005-0107	High	Debian Security Advisory, DSA 690-1, February 25, 2005

Multiple Vendors Daniel Stenberg curl 6.0-6.4, 6.5-6.5.2, 7.1, 7.1.1, 7.2, 7.2.1, 7.3, 7.4, 7.4.1, 7.10.1, 7.10.3-7.10.7, 7.12.1	A buffer overflow vulnerability exists in the Kerberos authentication code in the 'Curl_krb_kauth()' and 'krb4_auth()' functions and in the NT Lan Manager (NTLM) authentication in the 'Curl_input_ntlm()' function, which could let a remote malicious user execute arbitrary code. **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** **Ubuntu:** **http://security.ubuntu.com/ ubuntu/pool/main/c/curl/** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendors cURL / libcURL Kerberos Authentication & 'Curl_input_ntlm()' Remote Buffer Overflows CAN-2005-0490	High	iDEFENSE Security Advisory, February 21, 2005 **SUSE Security Announcements, SUSE-SR:2005:006 & SUSE-SA:2005:011, February 25 & 28, 2005** **Ubuntu Security Notice, USN-86-1, February 28, 2005**
Multiple Vendors FileZilla Server 0.7, 0.7.1; OpenBSD -current, 3.5; OpenPKG Current, 2.0, 2.1; zlib 1.2.1	A remote Denial of Service vulnerability exists during the decompression process due to a failure to handle malformed input. Gentoo: http://security.gentoo.org/glsa/ glsa-200408-26.xml FileZilla: http://sourceforge.net/project/showfiles. php?group_id=21558 OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/ 3.5/common/017_libz.patch OpenPKG: ftp ftp.openpkg.org Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ SuSE: ftp://ftp.suse.com/pub/suse/ Mandrake: http://www.mandrakesecure.net/ en/ftp.php Conectiva: ftp://atualizacoes.conectiva.com.br/ SCO: ftp://ftp.sco.com/pub/updates/ UnixWare/SCOSA-2004.17 Fedora: http://download.fedora.redhat.com /pub/fedora/linux/core/updates/2/ **FedoraLegacy:** **http://download.fedoralegacy.org/ fedora/1/updates/** We are not aware of any exploits for this vulnerability.	Zlib Compression Library Remote Denial of Service CAN-2004-0797	Low	SecurityFocus, August 25, 2004 SUSE Security Announcement, SUSE-SA:2004:029, September 2, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:090, September 8, 2004 Conectiva Linux Security Announcement, CLA-2004:865, September 13, 2004 US-CERT VU#238678, October 1, 2004 SCO Security Advisory, SCOSA-2004.17, October 19, 2004 Conectiva Linux Security Announcement, CLA-2004:878, October 25, 2004 Fedora Update Notification, FEDORA-2005-095, January 28, 2005 **Fedora Legacy Update Advisory, FLSA:2043, February 24, 2005**
Multiple Vendors GNU Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; GNOME gdk-pixbug 0.22 & prior; GTK GTK+ 2.0.2, 2.0.6, 2.2.1, 2.2.3, 2.2.4; MandrakeSoft Linux Mandrake 9.2, amd64, 10.0, AMD64; RedHat Advanced Workstation for the Itanium Processor 2.1, IA64, Desktop 3.0, Enterprise Linux WS 3, WS 2.1 IA64, WS 2.1, ES 3, ES 2.1 IA64, ES 2.1, AS 3, AS 2.1 IA64, AS 2.1, RedHat Fedora Core1&2; SuSE. Linux 8.1, 8.2, 9.0, x86_64, 9.1,	Multiple vulnerabilities exist: a vulnerability exists when decoding BMP images, which could let a remote malicious user cause a Denial of Service; a vulnerability exists when decoding XPM images, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and a vulnerability exists when attempting to decode ICO images, which could let a remote malicious user cause a Denial of Service. Debian: http://security.debian.org/pool/ updates/main/g/gdk-pixbuf/ Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ SuSE: ftp://ftp.suse.com/pub/suse/ Gentoo: http://security.gentoo.org/glsa/ glsa-200409-28.xml Conectiva: ftp://atualizacoes.conectiva.com.br/	gdk-pixbug BMP, ICO, and XPM Image Processing Errors CAN-2004-0753 CAN-2004-0782 CAN-2004-0783 CAN-2004-0788	Low/High (High if arbitrary code can be executed)	SecurityTracker Alert ID, 1011285, September 17, 2004 Gentoo Linux Security Advisory, GLSA 200409-28, September 21, 2004 US-CERT VU#577654, VU#369358, VU#729894, VU#825374, October 1, 2004 Conectiva Linux Security Announcement, CLA-2004:875, October 18, 2004 **Fedora Legacy Update Advisory, FLSA:2005, February 24, 2005**

Desktop 1.0, Enterprise Server 9, 8	**Fedora:** **http://download.fedoralegacy.org/redhat/** We are not aware of any exploits for these vulnerabilities.			
Multiple Vendors Larry Wall Perl 5.8, 5.8.1, 5.8.3, 5.8.4, 5.8.4 -1-5.8.4-5; Ubuntu Linux 4.1 ppc, ia64, ia32	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'PERLIO_DEBUG' SuidPerl environment variable, which could let a malicious user execute arbitrary code; and a vulnerability exists due to an error when handling debug message output, which could let a malicious user corrupt arbitrary files. Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/p/perl/ Gentoo: http://security.gentoo.org/glsa/glsa-200502-13.xml Mandrake: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:031 RedHat: http://rhn.redhat.com/errata/RHSA-2005-105.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ SUSE: ftp://ftp.suse.com/pub/suse/ Trustix: http://www.trustix.org/errata/2005/0003/ **IBM:** **ftp://aix.software.ibm.com/aix/efixes/security/perl58x.tar.Z** Proofs of Concept exploits have been published.	Perl SuidPerl Multiple Vulnerabilities CAN-2005-0155 CAN-2005-0156	Medium/ High (High if arbitrary code can be executed)	Ubuntu Security Notice, USN-72-1, February 2, 2005 MandrakeSoft Security Advisory, MDKSA-2005:031, February 9, 2005 RedHat Security Advisory, RHSA-2005:105-11, February 7, 2005 SGI Security Advisory, 20050202-01-U, February 9, 2005 SUSE Security Summary Report, SUSE-SR:2005:004, February 11, 2005 Gentoo Linux Security Advisory, GLSA 200502-13, February 11, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0003,February 11, 2005 **IBM SECURITY ADVISORY, February 28, 2005**
Multiple Vendors Linux Kernel 2.2, 2.4, 2.6	Several buffer overflow vulnerabilities exist in 'drivers/char/moxa.c' due to insufficient validation of user-supplied inputs to the 'MoxaDriverIoctl(),' ' moxaloadbios(),' moxaloadcode(),' and 'moxaload320b()' functions, which could let a malicious user execute arbitrary code with root privileges. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Moxa Char Driver Buffer Overflows CAN-2005-0504	High	SecurityTracker Alert, 1013273, February 23, 2005
Multiple Vendors Linux kernel 2.2-2.2.2.27 -rc1, 2.4-2.4.29 -rc1, 2.6 .10, 2.6- 2.6.10	A race condition vulnerability exists in the page fault handler of the Linux Kernel on symmetric multiprocessor (SMP) computers, which could let a malicious user obtain superuser privileges. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **SuSE:** **ftp://ftp.suse.com/pub/suse/** RedHat: http://rhn.redhat.com/errata/RHSA-2005-016.html http://rhn.redhat.com/errata/RHSA-2005-017.html Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html **FedoraLegacy:**	Linux Kernel Symmetrical Multiprocessing Page Fault Superuser Privileges CAN-2005-0001	High	SecurityTracker Alert, 1012862, January 12, 2005 SUSE Security Announcement, SUSE-SA:2005:003, January 21, 2005 RedHat Security Advisory, RHSA-2005:016-13 & 017-14, January 21, 2005 Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 **Fedora Legacy Update Advisory, FLSA:2336, February 24, 2005** **SUSE Security Announcement, SUSE-SA:2005:010, February 25, 2005** **Turbolinux Security Announcement , February 28, 2005**

	http://download.fedoralegacy.org/redhat/ **SuSE:** **ftp://ftp.suse.com/pub/suse/** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/** Exploit scripts have been published.			
Multiple Vendors Linux kernel 2.4 .0-test1-test12, 2.4-2.4.27; Avaya Converged Communications Server 2.0, Avaya Intuity LX, Avaya MN100, Avaya Modular Messaging (MSS) 1.1, 2.0, Avaya Network Routing Avaya S8300 R2.0.1, R2.0.0, S8500 R2.0.1, R2.0.0, S8700 R2.0.1, R2.0.0, S8710 R2.0.1, R2.0.0	A vulnerability exists in the 'AF_UNIX' address family due to a serialization error, which could let a malicious user obtain elevated privileges or possibly execute arbitrary code. Upgrades available at: http://kernel.org/pub/linux/kernel/v2.4/linux-2.4.28.tar.bz2 SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main Red Hat: http://rhn.redhat.com/errata/RHSA-2004-504.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-006_RHSA-2004-549RHSA-2004-505RHSA-2004-689.pdf Mandrake: http://www.mandrakesecure.net/en/ftp.php **FedoraLegacy: http://download.fedoralegacy.org/redhat/** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel AF_UNIX Arbitrary Kernel Memory Modification CAN-2004-1068	Medium/ High (High if arbitrary code can be executed)	Bugtraq, November 19, 2004 SUSE Security Summary Report, SUSE-SR:2004:003, December 7, 2004 SecurityFocus, December 14, 2004 Fedora Update Notifications, FEDORA-2004-581 & 582, January 4, 2005 Avaya Security Advisory, ASA-2005-006, January 14, 2006 Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005 **Fedora Legacy Update Advisory, FLSA:2336, February 24, 2005** **Turbolinux Security Announcement , February 28, 2005**
Multiple Vendors Linux kernel 2.4 .0-test1-test12, 2.4-2.4.28, 2.4.29 -rc1&rc2, 2.6 -test1-test11, 2.6-2.6.10, 2.6.10 rc1; RedHat Desktop 3.0, Enterprise Linux WS 3, Linux ES 3, Linux AS 3; S.u.S.E. Linux 8.1, 8.2, 9.0-9.2, Linux Desktop 1.0, Linux Enterprise Server 9, 8, Novell Linux Desktop 9.0	A Denial of Service vulnerability exists in the audit subsystem of the Linux kernel. . RedHat: http://rhn.redhat.com/errata/RHSA-2005-043. **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Audit Subsystem Denial of Service CAN-2004-1237	Low	RedHat Security Advisory, RHSA-2005:043-13, January 18, 2005 SUSE Security Announcement, SUSE-SA:2005:003, January 21, 2005 **SUSE Security Announcement, SUSE-SA:2005:010, February 25, 2005**

Multiple Vendors Linux Kernel 2.4.0 test1-test12, 2.4-2.4.28, 2.4.29 -rc2, 2.6, test1-test11, 2.6.1, rc1-rc2, 2.6.2-2.6.9, 2.6.10 rc2; Avaya S8710/S8700/ S8500/S8300, Converged Communication Server, Intuity LX, MN100, Modular Messaging, Network Routing	A vulnerability exists in the 'load_elf_library()' function in 'binfmt_elf.c' because memory segments are not properly processed, which could let a remote malicious user execute arbitrary code with root privileges. Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/l/ Mandrake: http://www.mandrakesecure.net/ en/ftp.php Avaya: http://support.avaya.com/elmodocs2/ security/ASA-2005-034_RHSA-2005 -016RHSA-2006-017RHSA-2005-043.pdf Ubuntu: http://security.ubuntu.com/ubuntu/ pool/main/l/linux-source-2.6.8.1/ RedHat: https://rhn.redhat.com/errata/ RHSA-2005-092.html **FedoraLegacy:** **http://download.fedoralegacy. org/redhat/** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/** Another exploit script has been published.	Linux Kernel uselib() Root Privileges CAN-2004-1235	High	iSEC Security Research Advisory, January 7, 2005 Fedora Update Notifications, FEDORA-2005-013 & 014, January 10, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0001, January 13, 2005 Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005 PacketStorm, January 27, 2005 Avaya Security Advisory, ASA-2005-034, February 8, 2005 Ubuntu Security Notice, USN-57-1, February 9, 2005 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 **Fedora Legacy Update Advisory, FLSA:2336, February 24, 2005** **SUSE Security Announcement, SUSE-SA:2005:010, February 25, 2005** **Turbolinux Security Announcement , February 28, 2005**
Multiple Vendors Linux kernel 2.4.0-test1-test12, 2.4-2.4.28, 2.4.29 -rc1&rc2	A vulnerability exists in the processing of ELF binaries on IA64 systems due to improper checking of overlapping virtual memory address allocations, which could let a malicious user cause a Denial of Service or potentially obtain root privileges. Patch available at: http://linux.bkbits.net:8080/linux-2.6/cset@ 41a6721cce-LoPqkzKXudYby_3TUmg Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ RedHat: http://rhn.redhat.com/errata/ RHSA-2005-043.html http://rhn.redhat.com/errata/ RHSA-2005-017.html Mandrake: http://www.mandrakesecure.net/ en/ftp.php **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Overlapping VMAs CAN-2005-0003	Low/High (High if root access can be obtained)	Trustix Secure Linux Security Advisory, TSLSA-2005-0001, January 13, 2005 RedHat Security Advisories, RHSA-2005:043-13 & RHSA-2005:017-14m January 18 & 21, 2005 Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005 **Turbolinux Security Announcement , February 28, 2005**
Multiple Vendors Linux Kernel 2.4-2.4.27, 2.6-2.6.8 SUSE Linux 8.1, 8.2, 9.0, 9.1, Linux 9.2, SUSE Linux Desktop 1.x, SUSE Linux Enterprise Server 8, 9; Avaya Converged Communications Server 2.0, Avaya Intuity LX, Avaya MN100,	Multiple vulnerabilities exist due to various errors in the 'load_elf_binary' function of the 'binfmt_elf.c' file, which could let a malicious user obtain elevated privileges and potentially execute arbitrary code. Patch available at: http://linux.bkbits.net:8080/ linux-2.6/gnupatch@41925edcVccs XZXObG444GFvEJ94GQ Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/	Multiple Vendors Linux Kernel BINFMT_ELF Loader Multiple Vulnerabilities CAN-2004-1070 CAN-2004-1071 CAN-2004-1072 CAN-2004-1073	Medium/ High (High if arbitrary code can be executed)	Bugtraq, November 11, 2004 Fedora Update Notifications, FEDORA-2004-450 & 451, November 23, 2004 SUSE Security Summary Report, SUSE-SA:2004:042, December 1, 2004 Red Hat Advisory:

Avaya Modular Messaging (MSS) 1.1, 2.0, Avaya Network Routing Avaya S8300 R2.0.1, R2.0.0, S8500 R2.0.1, R2.0.0, S8700 R2.0.1, R2.0.0, S8710 R2.0.1, R2.0.0	pub/fedora/linux/core/updates/ SUSE: http://www.SUSE.de/de/security/2004_42_kernel.html Red Hat: http://rhn.redhat.com/errata/RHSA-2004-549.html RedHat: http://rhn.redhat.com/errata/RHSA-2004-504.html http://rhn.redhat.com/errata/RHSA-2004-505.html Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-006_RHSA-2004-549 RHSA-2004-505RHSA-2004-689.pdf Mandrake: http://www.mandrakesecure.net/en/ftp.php **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** Proofs of Concept exploit scripts have been published.			RHSA-2004:549-10, December 2, 2004 RedHat Security Advisories, RHSA-2004:504-13 & 505-14, December 13, 2004 Avaya Security Advisory, ASA-2005-006, January 14, 2006 Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005 **Fedora Legacy Update Advisory, FLSA:2336, February 24, 2005**
Multiple Vendors Linux Kernel 2.4-2.4.27, 2.6-2.6.9; Trustix Secure Enterprise Linux 2.0, Secure Linux 1.5, 2.0-2.2; Ubuntu Linux 4.1 ppc, 4.1 ia64, 4.1 ia32; SUSE Linux 8.1, 8.2, 9.0, 9.1, Linux 9.2, SUSE Linux Desktop 1.x, SUSE Linux Enterprise Server 8, 9	Multiple remote Denial of Service vulnerabilities exist in the SMB filesystem (SMBFS) implementation due to various errors when handling server responses. This could also possibly lead to the execution of arbitrary code. Upgrades available at: http://kernel.org/pub/linux/kernel/v2.4/linux-2.4.28.tar.bz2 Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: http://www.SUSE.de/de/security/2004_42_kernel.html Red Hat: http://rhn.redhat.com/errata/RHSA-2004-549.html RedHat: http://rhn.redhat.com/errata/RHSA-2004-504.html http://rhn.redhat.com/errata/RHSA-2004-505.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Mandrake: http://www.mandrakesecure.net/en/ftp.php **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/** Currently we are not aware of any exploits for these vulnerabilities	Multiple Vendors smbfs Filesystem Memory Errors Remote Denial of Service CAN-2004-0883 CAN-2004-0949	Low/High (High if arbitrary code can be executed)	e-matters GmbH Security Advisory, November 11, 2004 Fedora Update Notifications, FEDORA-2004-450 & 451, November 23, 2004 SUSE Security Summary Report, SUSE-SA:2004:042, December 1, 2004 Red Hat Advisory: RHSA-2004:549-10, December 2, 2004 Ubuntu Security Notice, USN-39-1, December 16, 2004 RedHat Security Advisories, RHSA-2004:504-13 & 505-14, December 13, 2004 SUSE Security Announcement, SUSE-SA:2005:003, January 21, 2005 Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005 US-CERT VU#726198, February 1, 2005 **Fedora Legacy Update Advisory, FLSA:2336, February 24, 2005** **SUSE Security Announcement, SUSE-SA:2005:010, February 25, 2005** **Turbolinux Security Announcement , February 28, 2005**

Multiple Vendors Linux Kernel 2.6 - 2.6.10 rc2	The DRM module in the Linux kernel is susceptible to a local Denial of Service vulnerability. This vulnerability likely results in the corruption of video memory, crashing the X server. Malicious users may be able to modify the video output. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel Local DRM Denial of Service CAN-2004-1056	Low	Ubuntu Security Notice USN-38-1 December 14, 2004 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 **Fedora Legacy Update Advisory, FLSA:2336, February 24, 2005**
Multiple Vendors Linux Kernel 2.6 - 2.6.10 rc2	The Linux kernel /proc filesystem is susceptible to an information disclosure vulnerability. This issue is due to a race-condition allowing unauthorized access to potentially sensitive process information. This vulnerability may allow malicious local users to gain access to potentially sensitive environment variables in other users processes. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main Mandrake: http://www.mandrakesecure.net/en/ftp.php **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel PROC Filesystem Local Information Disclosure CAN-2004-1058	Medium	Ubuntu Security Notice USN-38-1 December 14, 2004 Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005 **Turbolinux Security Announcement , February 28, 2005**
Multiple Vendors Linux Kernel 2.6 - 2.6.10 rc2	The Linux kernel is prone to a local Denial of Service vulnerability. This vulnerability is reported to exist when 'CONFIG_SECURITY_NETWORK=y' and 'CONFIG_SECURITY_SELINUX=y' options are set in the Linux kernel. A local attacker may exploit this vulnerability to trigger a kernel panic and effectively deny service to legitimate users. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Mandrake: http://www.mandrakesecure.net/en/ftp.php **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel Sock_DGram_SendMsg Local Denial of Service CAN-2004-1069	Low	Ubuntu Security Notice USN-38-1 December 14, 2004 Fedora Update Notifications, FEDORA-2004-581 & 582, January 4, 2005 Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005 **Turbolinux Security Announcement , February 28, 2005**
Multiple Vendors Linux Kernel 2.6 .10, 2.6, test-test11, 2.6.1-2.6.10, 2.6.10 rc2; RedHat Fedora Core2&3	An integer overflow vulnerability exists in the 'scsi_ioctl.c' kernel driver due to insufficient sanitization of the 'sg_scsi_ioctl' function, which could let a malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **SuSE:** **ftp://ftp.suse.com/pub/suse/** RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html Currently we are not aware of any exploits for this vulnerability.	Linux Kernel SCSI IOCTL Integer Overflow CAN-2005-0180	High	Bugtraq, January 7, 2005 Fedora Update Notifications, FEDORA-2005-013 & 014, January 10, 2005 SUSE Security Announcement, SUSE-SA:2005:003, January 21, 2005 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 **SUSE Security Announcement, SUSE-SA:2005:010, February 25, 2005**

Multiple Vendors Linux kernel 2.6 -test1-test11, 2.6-l 2.6.8; SuSE Linux 9.1	A remote Denial of Service vulnerability exists in the iptables logging rules due to an integer underflow. Update available at: http://kernel.org/ SuSE: ftp://ftp.suse.com/pub/suse/ Mandrake: http://www.mandrakesecure.net /en/ftp.php **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/** A Proof of Concept exploit script has been published.	Linux Kernel IPTables Logging Rules Remote Denial of Service CAN-2004-0816	Low	SuSE Security Announcement, SUSE-SA:2004:037, October 20, 2004 Packetstorm, November 5, 2004 Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005 **Turbolinux Security Announcement , February 28, 2005**
Multiple Vendors Linux kernel 2.6.10, 2.6 -test9-CVS, 2.6-test1- -test11, 2.6, 2.6.1-2.6.11 ; RedHat Desktop 4.0, Enterprise Linux WS 4, ES 4, AS 4	Multiple vulnerabilities exist: a vulnerability exists in the 'shmctl' function, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists in 'nls_ascii.c' due to the use of incorrect table sizes; a race condition vulnerability exists in the 'setsid()' function; and a vulnerability exists in the OUTS instruction on the AMD64 and Intel EM64T architecture, which could let a malicious user obtain elevated privileges. RedHat: https://rhn.redhat.com/errata/ RHSA-2005-092.html Ubuntu: http://security.ubuntu.com/ubuntu/ pool/main/l/linux-source-2.6.8.1/ **FedoraLegacy:** **http://download.fedoralegacy. org/redhat/** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Multiple Vulnerabilities CAN-2005-0176 CAN-2005-0177 CAN-2005-0178 CAN-2005-0204	Low/Medium (Low if a DoS)	Ubuntu Security Notice, USN-82-1, February 15, 2005 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 **Fedora Legacy Update Advisory, FLSA:2336, February 24, 2005**
Multiple Vendors Linux kernel 2.6.x, 2.4.x , SUSE Linux 8.1, 8.2, 9.0, 9.1, Linux 9.2, SUSE Linux Desktop 1.x, SUSE Linux Enterprise Server 8, 9; Turbolinux Turbolinux Server 10.0	Two vulnerabilities exist: a Denial of Service vulnerability exists via a specially crafted 'a.out' binary; and a vulnerability exists due to a race condition in the memory management, which could let a malicious user obtain sensitive information. SUSE: http://www.SUSE.de/de/security/2004_42_ kernel.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/ TurboLinux/ia32/Server/10/updates/RPMS/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Trustix: http://http.trustix.org/pub/trustix/updates/ Mandrake: http://www.mandrakesecure.net/ en/ftp.php **FedoraLegacy:** **http://download.fedoralegacy. org/redhat/** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendors Linux Kernel Local DoS & Memory Content Disclosure CAN-2004-1074	**Low/ Medium** **(Medium if sensitive information can be obtained)**	Secunia Advisory, SA13308, November 25, 2004 SUSE Security Summary Report, SUSE-SA:2004:042, December 1, 2004 SecurityFocus, December 16, 2004 Trustix Secure Linux Security Advisory, TSLSA-2005-0001, January 13, 2005 Mandrake Security Advisory, MDKSA-2005:022, January 26, 2005 **Fedora Legacy Update Advisory, FLSA:2336, February 24, 2005**
Multiple Vendors Linux Kernel USB Driver prior to 2.4.27; Avaya Converged Communications Server 2.0, Avaya Intuity LX, Avaya MN100, Avaya Modular Messaging (MSS) 1.1, 2.0, Avaya Network Routing Avaya S8300 R2.0.1, R2.0.0, S8500 R2.0.1, R2.0.0, S8700 R2.0.1, R2.0.0, S8710 R2.0.1,	A vulnerability exists in certain USB drivers because uninitialized structures are used and then 'copy_to_user(...)' kernel calls are made from these structures, which could let a malicious user obtain obtain uninitialized kernel memory contents. Update available at: http://kernel.org/ Gentoo: http://www.gentoo.org/security/ en/glsa/glsa- 200408-24.xml Trustix: http://http.trustix.org/pub/ trustix/updates/ Red Hat: http://rhn.redhat.com/errata/ RHSA-2004-504.html	Multiple Vendors Linux Kernel USB Driver Kernel Memory CAN-2004-0685	Medium	US-CERT VU#981134, October 25, 2004 Trustix, TSLSA-2004-0041: kernel, August 9, 2004 Red Hat Security Advisories, RHSA-2004:505-14 & 505-13, December 13, 2004 Avaya Security Advisory, ASA-2005-006, January 14, 2006 **Fedora Legacy Update Advisory, FLSA:2336, February 24, 2005**

R2.0.0	Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-006_RHSA-2004-549RHSA-2004-505RHSA-2004-689.pdf **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** We are not aware of any exploits for this vulnerability.			
Multiple Vendors Linux Kernel; Avaya Converged Communications Server 2.0, Avaya Intuity LX, Avaya MN100, Avaya Modular Messaging (MSS) 1.1, 2.0, Avaya Network Routing Avaya S8300 R2.0.1, R2.0.0, S8500 R2.0.1, R2.0.0, S8700 R2.0.1, R2.0.0, S8710 R2.0.1, R2.0.0	A vulnerability exists in the Linux kernel io_edgeport driver. A local user with a USB dongle can cause the kernel to crash or may be able to gain elevated privileges on the target system. The flaw resides in the edge_startup() function in 'drivers/usb/serial/io_edgeport.c'. Red Hat: https://bugzilla.redhat.com/bugzilla/attachment.cgi?id=107493&action=view Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-006_RHSA-2004-549RHSA-2004-505RHSA-2004-689.pdf **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel USB io_edgeport Driver Integer Overflow CAN-2004-1017	Low/ Medium (Medium if elevated privileges can be obtained)	SecurityTracker Alert ID: 1012477, December 10, 2004 Fedora Update Notifications, FEDORA-2004-581 & 582, January 3, 2005 Avaya Security Advisory, ASA-2005-006, January 14, 2005 **Fedora Legacy Update Advisory, FLSA:2336, February 24, 2005**
Multiple Vendors PHP 4.0.1-4.0.7, PHP PHP 4.1 .0-4.1.2, 4.2 .0-4.2.3, 4.3-4.3.10; SuSE Linux 9.0 x86_64, 9.0, 9.1 x86_64, 9.1, Linux Enterprise Server 9	A Denial of Service vulnerability exists in the 'readfile()' function. SuSE: ftp://ftp.suse.com/pub/suse/ There is no exploit code required.	PHP4 'readfile()' Denial of Service CAN-2005-0596	Low	SUSE Security Summary Report, ID: SUSE-SR:2005:006, February 25, 2005
NoMachine NX Server 1.3-1.3.2	Several vulnerabilities exist: a vulnerability exists in the authority file due to an error in the way the file is handled, which could let a malicious user bypass authentication; and a vulnerability exists in the authority file when it is read and interrupted by a signal, which could let a malicious user bypass authentication. Update available at: http://www.nomachine.com/download.php SUSE: ftp://ftp.SUSE.com/pub/SUSE Currently we are not aware of any exploits for these vulnerability.	NX Server X Server Authentication Bypass	Medium	Secunia Advisory, SA14417, February 28, 2005 SUSE Security Summary Report, SUSE-SR:2005:006, February 25, 2005
Rob Flynn Gaim 1.0-1.0.2, 1.1.1, 1.1.2	Multiple remote Denial of Service vulnerabilities exist: a vulnerability exists when a remote malicious ICQ or AIM user submits certain malformed SNAC packets; and a vulnerability exists when parsing malformed HTML data. Upgrades available at: http://gaim.sourceforge.net/downloads.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/g/gaim/** There is no exploit code required.	Gaim Multiple Remote Denials of Service CAN-2005-0472 CAN-2005-0473	Low	Gaim Advisory, February 17, 2005 Fedora Update Notifications, FEDORA-2005-159 & 160, February 21, 2005 US-CERT VU#839280 US-CERT VU#523888 **Ubuntu Security Notice, USN-85-1 February 25, 2005**
SCO Open Server 5.0-5.0.7	A buffer overflow vulnerability exists in the scosession due to insufficient validation of user-supplied input strings prior to copying them to finite process buffers, which could let a malicious user execute arbitrary code. Updates available at: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.5 Currently we are not aware of any exploits for this vulnerability.	SCO scosession Buffer Overflow CAN-2003-1021	High	SCO Security Advisory, SCOSA-2005.5, January 26, 2005 **US-CERT VU#972598**

Squid-cache.org Squid Web Proxy Cache 2.5 .STABLE5-STABLE8	A remote Denial of Service vulnerability exists when performing a Fully Qualify Domain Name (FQDN) lookup and and unexpected response is received. Patches available at: http://downloads.securityfocus.com/vulnerabilities/patches/ Gentoo: http://security.gentoo.org/glsa/glsa-200502-25.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **Debian:** **http://security.debian.org/pool/updates/main/s/squid/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for this vulnerability.	Squid Proxy FQDN Remote Denial of Service CAN-2005-0446	Low	Secunia Advisory, SA14271, February 14, 2005 Gentoo Linux Security Advisory GLSA, 200502-25, February 18, 2005 Ubuntu Security Notice, USN-84-1, February 21, 2005 Fedora Update Notifications, FEDORA-2005-153 & 154, February 21, 2005 SUSE Security Announcement, SUSE-SA:2005:008, February 21, 2005 **Debian Security Advisory, DSA 688-1, February 23, 2005** **Mandrakelinux Security Update Advisory, MDKSA-2005:047, February 24, 2005**
Sun Microsystems, Inc. Solaris 9.0 _x86, 9.0	A Denial of Service vulnerability exists in the Standard Type Services Framework Font Server Daemon (stfontserverd). Patches available at: http://classic.sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=117202&rev=09 Currently we are not aware of any exploits for this vulnerability.	Sun Solaris STFontServerD Denial of Service CAN-2005-0576	Low	Sun(sm) Alert Notification, 57738, February 24, 2005
Typespeed Typespeed 0.4.1	A local format string vulnerability exists which could let a malicious user obtain elevated privileges. Debian: http://security.debian.org/pool/updates/main/t/typespeed/ **Proof of Concept exploit script has been published.**	Typespeed Format String CAN-2005-0105	Medium	Debian Security Advisory DSA 684-1, February 16, 2005 **PacketStorm, February 25, 2005**
Uim Uim 4.5	A vulnerability exists in the Uim library because environment variables contents are always trusted, which could let a malicious user obtain elevated privileges. Upgrade available at: http://uim.freedesktop.org/releases/uim-0.4.5.1.tar.gz **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200502-31.xml** Currently we are not aware of any exploits for this vulnerability.	UIM LibUIM Elevated Privileges CAN-2005-0503	Medium	SecurityFocus, 12604, February 21, 2005 **Mandrakelinux Security Update Advisory, MDKSA-2005:046, February 24, 2005** **Gentoo Linux Security Advisory, GLSA 200502-31, February 28, 2005**

University of Washington imap 2004b, 2004a, 2004, 2002b-2002e	A vulnerability exists due to a logic error in the Challenge-Response Authentication Mechanism with MD5 (CRAM-MD5) code, which could let a remote malicious user bypass authentication. Update available at: ftp://ftp.cac.washington.edu/mail/imap-2004b.tar.Z Gentoo: http://security.gentoo.org/glsa/glsa-200502-02.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-128.html** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	University Of Washington IMAP Server CRAM-MD5 Remote Authentication Bypass CAN-2005-0198	Medium	US-CERT VU#702777, January 27, 2005 Gentoo Linux Security Advisory, GLSA 200502-02, February 2, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:026, February 2, 2005 **RedHat Security Advisory, RHSA-2005:128-06, February 23, 2005** **SUSE Security Announcements, SUSE-SR:2005:006 & SUSE-SA:2005:012, February 25 & March 1, 2005**
VIM Development Group VIM 6.0-6.2, 6.3.011, 6.3.025, 6.3 .030, 6.3.044, 6.3 .045	Multiple vulnerabilities exist in 'tcltags' and 'vimspell.sh' due to the insecure creation of temporary files, which could let a malicious user corrupt arbitrary files. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/v/vim/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-122.html **Fedora:** **http://download.fedoralegacy.org/redhat/** There is no exploit required.	Vim Insecure Temporary File Creation CAN-2005-0069	Medium	Secunia Advisory, SA13841, January 13, 2005 Ubuntu Security Notice, USN-61-1, January 18, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:026, February 2, 200 **Fedora Legacy Update Advisory, FLSA:2343, February 24, 2005**
winace.com UnAce 1.0, 1.1, 1.2 b	Several vulnerabilities exist: a buffer overflow vulnerability exists in the ACE archive due to an incorrect 'strncpy()' call, which could let a remote malicious user execute arbitrary code; two other buffer overflow vulnerabilities exist when archive name command line arguments are longer than 15,600 characters and when printing strings are processed, which could let a remote malicious user execute code; and a Directory Traversal vulnerability exists due to improper filename character processing, which could let a remote malicious user obtain sensitive information. Gentoo: http://security.gentoo.org/glsa/glsa-200502-32.xml There is not exploit code required; however, Proofs of Concept exploits have been published.	Winace UnAce ACE Archive Remote Directory Traversal & Buffer Overflow CAN-2005-0160 CAN-2005-0161	Medium/ High (High if arbitrary code can be executed)	SecurityTracker Alert, 1013265, February 23, 2005
xmlsoft.org Libxml2 2.6.12-2.6.14	Multiple buffer overflow vulnerabilities exist: a vulnerability exists in the 'xmlNanoFTPScanURL()' function in 'nanoftp.c' due to a boundary error, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'xmlNanoFTPScanProxy()' function in 'nanoftp.c,' which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the handling of DNS replies due to various boundary errors, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://xmlsoft.org/sources/libxml2-2.6.15.tar.gz OpenPKG: ftp://ftp.openpkg.org/release/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-05.xml	xmlsoft.org Libxml2 Multiple Remote Stack Buffer Overflows CAN-2004-0989 CAN-2004-0110	High	SecurityTracker Alert I, 1011941, October 28, 2004 Fedora Update Notification, FEDORA-2004-353, November 2, 2004 Gentoo Linux Security Advisory, GLSA 200411-05, November 2,2 004 Mandrakelinux Security Update Advisory, MDKSA-2004:127, November 4, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.050, November 1, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0055, November 1, 2004

	Mandrake: http://www.mandrakesoft.com/security/advisories OpenPKG: ftp://ftp.openpkg.org/release/ Trustix: http://www.trustix.org/errata/2004/0055/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libx/libxml2/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-615.html Conectiva: ftp://atualizacoes.conectiva.com.br/1 RedHat (libxml): http://rhn.redhat.com/errata/RHSA-2004-650.html Apple: http://www.apple.com/support/downloads/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/libx/libxml/** An exploit script has been published.		Ubuntu Security Notice, USN-10-1, November 1, 2004 Red Hat Security Advisory, RHSA-2004:615-11, November 12, 2004 Conectiva Linux Security Announcement, CLA-2004:890, November 18, 2004 Red Hat Security Advisory, RHSA-2004:650-03, December 16, 2004 Apple Security Update, APPLE-SA-2005-01-25, January 26, 2005 Turbolinux Security Advisory, TLSA-2005-11, January 26, 2005 **Ubuntu Security Notice, USN-89-1, February 28, 2005**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Apache mod_python	A vulnerability exists in mod_python in the publisher handler that could permit a remote malicious user to view certain python objects. A remote user can submit a specially crafted URL to view the names and values of variables. Red Hat: http://rhn.redhat.com/errata/RHSA-2005-104.html Ubuntu: http://www.ubuntulinux.org/support/documentation/usn/usn-80-1 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200502-14.xml Trustix: http://www.trustix.org/errata/2005/0003/ **Debian:** **http://www.debian.org/security/2005/dsa-689** Currently we are not aware of any exploits for this vulnerability.	Apache mod_python Information Disclosure Vulnerability CAN-2005-0088	Medium	SecurityTracker Alert ID, 1013156, February 11, 2005 Red Hat RHSA-2005:104-03, February 10, 2005 Ubuntu, USN-80-1 February 11, 2005 Trustix #2005-0003, February 11, 2005 **Debian, DSA-689-1, February 23, 2005**
Appalachian State University phpWebSite 0.10.0 and prior	A vulnerability exists in the Announce module that could let a remote malicious user who has privileges to upload image files execute arbitrary commands. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Appalachian State phpWebSite Arbitrary Code Execution Vulnerability CAN-2005-0565	High	SecurityFocus, Bugtraq ID: 12653, February 25, 2005

Arkeia Arkeia Network Backup 5.3.x and prior	A buffer overflow vulnerability exists that could let a remote malicious user execute arbitrary code on the target system. The software does not properly validate 'type 77' request packets. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Arkeia Network Backup Access Vulnerability CAN-2005-0496	High	SecurityTracker Alert ID: 1013256, February, 22 2005
Cisco ACNS Software Version 4.2 and prior	Multiple vulnerabilities exist that could let remote users cause a Denial of Service. These are due to errors within the processing of TCP connections, IP packets, and network packets. he vulnerabilities affect devices configured as a transparent, forward, or reverse proxy server. A default password may also be available in the administrative account. Updates available: http://www.cisco.com/warp/public/707/cisco-sa-20050224-acnsdos.shtml Currently we are not aware of any exploits for these vulnerabilities.	Cisco ACNS Denial of Service Vulnerabilities CAN-2005-0601 CAN-2005-0600 CAN-2005-0599 CAN-2005-0598 CAN-2005-0597	Low	Cisco Security Advisory: 64069 Revision 1.0, February 24, 2005
Cisco Cisco IPVC-3510-MCU, Cisco IPVC-3520-GW-2B, Cisco IPVC-3520-GW-4B, Cisco IPVC-3520-GW-2, Cisco IPVC-3520-GW-4V, Cisco IPVC-3520-GW-2B2V, Cisco IPVC-3525-GW-1P, Cisco IPVC-3530-VTA	A vulnerability exists in some Cisco videoconferencing products that could permit a remote malicious user to gain control of the system using common default SNMP community strings. Cisco has issued a workaround available at: http://www.cisco.com/public/technotes/cisco-sa-20050202-ipvc.shtml **Revision 1.1: Added products to "Products Confirmed Not Vulnerable" list. Updated opening paragraph of "Obtaining Fixed Software" section.** **Revision 1.2:Added paragraph to "Workarounds" section.** Currently we are not aware of any exploits for this vulnerability.	Cisco IP/VC Remote Access	High	Cisco Security Advisory 63894, February 2, 2005 **Cisco Security Advisory 63894, Revision 1.2 & 1.2, February 23 & 25, 2005**
Cyclades Corporation AlterPath Manager 1.2.1 and prior	Multiple vulnerabilities exist that could let a local malicious user bypass security restrictions and disclose system information. This is due to errors in "consoleConnect.jsp," "saveUser.do, " and "/about.html" The vulnerabilities will reportedly be fixed in version 1.2.5. Currently we are not aware of any exploits for these vulnerabilities.	Cyclades AlterPath Manager Access Vulnerability CAN-2005-0540 CAN-2005-0541 CAN-2005-0542	Medium	CIRT Advisories 200502, 200503, 200501, February 23, 2005
Devellion Limited CubeCart 2.0 - 2.0.5	Multiple vulnerabilities exist that could let a remote user determine the installation path and conduct Cross-Site Scripting attacks. This is due to input validation errors in the 'admin/Settings.inc.php' script. A remote user can also directly call certain scripts to display the installation path. The vendor has issued a fixed version (2.0.6) to correct the path disclosure flaws but not the Cross-Site Scripting flaws, available at: http://www.cubecart.com/site/downloads/ A Proof of Concept exploit has been published.	Devellion CubeCart Cross-Site Scripting and Information Disclosure Vulnerabilities CAN-2005-0606 CAN-2005-0607	High	SecurityFocus, Bugtraq ID: 12658, February 25, 2005
Frederico Caldeira Knabben FCKeditor 2.0 RC2	A vulnerability exists that could let a remote user can upload arbitrary files to the target system. Systems running PHP-Nuke and Mambo may be affected. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Frederico Knabben FCKeditor May Permit Arbitrary File Upload	Medium	SecurityFocus, Bugtraq ID: 12676, February 28, 2005
GNU AWStats 6.3 and prior	Multiple vulnerabilities exist which could permit local malicious users to gain escalated privileges, disclose system information, and cause a Denial of Service. This is due to errors in "awstats.pl" and the "loadplugin" and "pluginmode" parameters input validation. The vulnerabilities have reportedly been fixed in the CVS repository. **An exploit script has been published.**	GNU AWStats Multiple Vulnerabilities CAN-2005-0435 CAN-2005-0436 CAN-2005-0437 CAN-2005-0438 **CAN-2005-0363**	Low/ Medium (Medium if sensitive information can be obtained or elevated privileges are obtained)	SecurityFocus, Bugtraq ID 12545, February 14, 2005 **US-CERT VU#259785**
GNU Gaim prior to 1.1.4	A vulnerability exists in the processing of HTML that could let a remote malicious user crash the Gaim client. This is due to a NULL pointer dereference. A fixed version (1.1.4) is available at: http://gaim.sourceforge.net/downloads.php Ubuntu: http://www.ubuntulinux.org/support/documentation/usn/usn-85-1	GNU Gaim Denial of Service Vulnerability CAN-2005-0208	Low	Sourceforge.net Gaim Vulnerability Note, February 24, 2005 US-CERT VU#523888

	Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ Currently we are not aware of any exploits for this vulnerability.			
GNU PBLang 4.65	Multiple vulnerabilities exist that could permit a remote malicious user to conduct Cross-Site Scripting attacks. This is due to improper input validation in the 'search.php' script. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GNU PBLang Cross-Site Scripting Vulnerability CAN-2005-0526	High	SecurityTracker Alert ID: 1013277, February 23, 2005
GNU PunBB 1.2.1	Multiple vulnerabilities exist that could let a remote malicious user inject SQL commands. This is due to input validation errors in the 'register.php', 'profile.php', and 'moderate.php' scripts. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GNU PunBB SQL Injection Vulnerability CAN-2005-0569 CAN-2005-0570 CAN-2005-0571	High	SecurityTracker Alert ID: 1013294, February 25, 2005
GNU WebMod 0.47 (Half-LifeDedicated Server plugin)	A vulnerability exists that could let a remote malicious user cause a Denial of Service or execute arbitrary code. This is due to a boundary error in the handling of POST data in "server.cpp". Update to version 0.48: http://djeyl.net/w.php Currently we are not aware of any exploits for this vulnerability.	GNU WebMod "Content-Length" Remote Code Execution Vulnerability CAN-2005-0608	Low/ High (High if arbitrary code can be executed)	SecurityFocus, Bugtraq ID: 12679, February 28, 2005
GPL ginp 0.x	A vulnerability exists that could let a remote malicious user gain knowledge of sensitive information. This is due to an input validation error that could permit a directory traversal attack. Update to version 0.22: http://sourceforge.net/project/ showfiles.php?group_id=105663 Currently we are not aware of any exploits for this vulnerability.	GPL ginp Information Disclosure Vulnerability CAN-2005-0538	Medium	SecurityFocus,12642, February 23, 2005
IBM Hardware Management Console (HMC)	A vulnerability exists that could let a local malicious users obtain escalated privileges. This is due to an error in the Guided Setup Wizard. Apply APAR MB00913 for Version 4 Release 2.0 and later: http://techsupport.services.ibm.com/ server/hmc/power5/fixes/v4r4.html Currently we are not aware of any exploits for this vulnerability.	IBM Hardware Management Console (HMC) Privilege Escalation Vulnerability CAN-2005-0539	Medium	Secunia SA14377, February 24, 2005
iGeneric iG Shop 1.2	A vulnerability exists that could let a remote malicious user inject SQL commands. This is due to improper input validation in the 'page.php' script. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	iGeneric iG Shop SQL Execution Vulnerability CAN-2005-0537	High	SecurityTracker Alert ID: 1013268, February, 23 2005
ImageGalleryPlugin 1.x (TWiki plugin)	A vulnerability exists that could let a remote malicious user inject arbitrary shell commands. This is because some configuration options can be manipulated. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	ImageGallery Twiki Plugin Shell Command Injection CAN-2005-0516	High	Secunia SA14384, February 25, 2005
Mitel Mitel Model 3300 ICP PBX (prior to 4.2.2.11)	A vulnerability exists in the web interface that could let a remote malicious user hijack sessions. This is because the web interface uses a predictable session ID number for authentication purposes. Update to version (4.2.2.11). A Proof of Concept exploit has been published.	Mitel 3300 ICP PBX Session Hijack Vulnerability CAN-2004-0944	Medium	Corsaire Security Advisory --c040817-002, February 28, 2005
Mitel Mitel Model 3300 ICP PBX (prior to 5.2)	A vulnerability exists in the web interface that could let a remote user deny service. A user could establish 50 sessions to consume all available web sessions. This is due to input validation errors in the 'esm_validate.asp' script. Update to version (5.2). A Proof of Concept exploit has been published.	Mitel 3300 ICP PBX Denial of Service Vulnerability CAN-2004-0945	Low	Corsaire Security Advisory --c040817-003, February 28, 2005
Mozilla Firefox 1.0	A vulnerability exists in the XPCOM implementation that could let a remote malicious user execute arbitrary code. The exploit can be automated in conjunction with other reported vulnerabilities so no user interaction is required. A fixed version (1.0.1) is available at: http://www.mozilla.org/products/firefox/all.html A Proof of Concept exploit has been published.	Mozilla Firefox Remote Code Execution Vulnerability CAN-2005-0527	High	SecurityTracker Alert ID: 1013301, February 25, 2005

Mozilla Mozilla 1.7.x and prior Mozilla Firefox 1.x and prior Mozilla Thunderbird 1.x and prior	Multiple vulnerabilities exist in Firefox, Mozilla and Thunderbird. These can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges and by malicious people to conduct spoofing attacks, disclose and manipulate sensitive information, and potentially compromise a user's system. Firefox: Update to version 1.0.1: http://www.mozilla.org/products/firefox/ Mozilla: The vulnerabilities have been fixed in the CVS repository and will be included in the upcoming 1.7.6 version. Thunderbird: The vulnerabilities have been fixed in the CVS repository and will be included in the upcoming 1.0.1 version. Fedora update for Firefox: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Currently we are not aware of any exploits for these vulnerabilities.	Mozilla / Firefox / Thunderbird Multiple Vulnerabilities CAN-2005-0255 CAN-2005-0584 CAN-2005-0585 CAN-2005-0587 CAN-2005-0588 CAN-2005-0589 CAN-2005-0590 CAN-2005-0592 CAN-2005-0593	Medium	Mozilla Foundation Security Advisories 2005-14, 15, 17, 18, 19, 20, 21, 24, 28
Mozilla Firefox 1.0	There are multiple vulnerabilities in Mozilla Firefox. A remote user may be able to cause a target user to execute arbitrary operating system commands in certain situations or access access content from other windows, including the 'about:config' settings. This is due to a hybrid image vulnerability that allows batch statements to be dragged to the desktop and because tabbed javascript vulnerabilities let remote users access other windows. A fix is available via the CVS repository **Fedora:** **ftp://aix.software.ibm.com/aix/efixes/security/perl58x.tar.Z** A Proof of Concept exploit has been published.	Mozilla Firefox Multiple Vulnerabilities CAN-2005-0230 CAN-2005-0231 CAN-2005-0232	High	SecurityTracker Alert ID: 1013108, February 8, 2005 **Fedora Update Notification, FEDORA-2005-182, February 26, 2005**
Mozilla Mozilla 1.7.3 for Linux, Mozilla 1.7.5 for Windows, and Mozilla Firefox 1.0	A vulnerability exists which can be exploited by malicious people to spoof the source displayed in the Download Dialog box. The problem is that long sub-domains and paths aren't displayed correctly, which therefore can be exploited to obfuscate what is being displayed in the source field of the Download Dialog box. **Upgrade available at:** **http://ftp.mozilla.org/pub/mozilla.org/firefox/releases/1.0.1/source/firefox-1.0.1-source.tar.bz2** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** Currently we are not aware of any exploits for this vulnerability.	Mozilla / Mozilla Firefox Download Dialog Source Spoofing **CAN-2005-0585**	Medium	Secunia SA13599, January 4, 2005 **Fedora Update Notification, FEDORA-2005-182, February 28, 2005**
Mozilla Mozilla 1.7.3 Mozilla Firefox 1.0 for Windows	A vulnerability exists that could let remote malicious users trick users into downloading malicious files. This is because the the browser uses the different criteria to determine the the file type when saving the downloaded file. Updated versions are available. Mozilla Firefox 1.0.1: http://www.mozilla.org/products/firefox/ Mozilla 1.7.5: http://www.mozilla.org/products/mozilla1.x/ Currently we are not aware of any exploits for this vulnerability.	Mozilla / Firefox Download Spoofing Vulnerability CAN-2005-0586	Medium	Secunia SA13258, March 1, 2005 Mozilla Foundation Security Advisory 2005-22
Mozilla Mozilla Firefox 1.0 and 1.0.1	A vulnerability exists that could let remote malicious users conduct Cross-Site Scripting attacks. This is due to missing URI handler validation when dragging an image with a "javascript:" URL to the address bar. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Mozilla Firefox Image Javascript URI Dragging Cross-Site Scripting Vulnerability CAN-2005-0591	High	Secunia SA14406, March 1, 2005
phpBB Group phpBB 2.0.12 and prior	A vulnerability exists that could let a remote malicious user bypass certain security restrictions. This is due to errors in sessiondata['autologinid'], auto_login_key, and viewtopic.php. Update to version 2.0.13. An exploit script has been published.	phpBB "autologinid" Security Bypass CAN-2005-0603	Medium	phpBB 2.0.13 Release Notes, February 27, 2005

phpBB Team phpBB 2.0.11	Multiple vulnerabilities exist which remote malicious users could exploit to disclose and delete sensitive information. This is due to errors in the avatar handling functions. Update to version 2.0.12: http://www.phpbb.com/downloads.php **Gentoo:** **http://security.gentoo.org/ glsa/glsa-200503-02.xml** Currently we are not aware of any exploits for these vulnerabilities.	phpBB Information Disclosure Vulnerability CAN-2005-0258 CAN-2005-0259	Medium	phpBB Advisory 265423, February 21, 2005 **Gentoo inux Security Advisory, GLSA 200503-02, March 1, 2005** **US-CERT VU#774686**
phpMyAdmin phpMyAdmin 2.6.1	Multiple vulnerabilities exist that could let remote users conduct Cross-Site Scripting attacks and disclose sensitive information. This is due to input validation errors in "select_server.lib.php", "display_tbl_links.lib.php", "theme_left.css.php", "theme_right.css.php", "phpmyadmin.css.php", and"database_interface.lib.php." Update to version 2.6.1-pl1: http://sourceforge.net/project/ showfiles.php?group_id=23067 A Proof of Concept exploit script has been published.	phpMyAdmin Cross-Site Scripting and Information Disclosure Vulnerabilities CAN-2005-0543 CAN-2005-0544 CAN-2005-0567	Medium/ High (High if arbitrary code can be executed)	Sourceforge.net, phpMyAdmin Project Tracker 1149383 and 1149381, February 22, 2005
PostNuke PostNuke 0.750, 0.760RC2	Vulnerabilities exist that could let a remote malicious user inject SQL commands. The following modules do not properly validate user input: pnadmin.php, past.php, dl-util.php, dl-s earch.php, admin.php, index.php. Updates are available at: http://news.postnuke.com/ Exploit scripts have been published.	PostNuke SQL Injection Vulnerability	High	SecurityTracker Alert ID: 1013324, February 28, 2005
Python SimpleXMLRPCServer 2.2 all versions, 2.3 prior to 2.3.5, 2.4	A vulnerability exists in the SimpleXMLRPCServer library module that could permit a remote malicious user to access internal module data, potentially executing arbitrary code. Python XML-RPC servers that use the register_instance() method to register an object without a _dispatch() method are affected. Patches for Python 2.2, 2.3, and 2.4, available at: http://python.org/security/ PSF-2005-001/patch-2.2.txt (Python 2.2) http://python.org/security/ PSF-2005-001/patch.txt (Python 2.3, 2.4) The vendor plans to issue fixed versions for 2.3.5, 2.4.1, 2.3.5, and 2.4.1. Debian: http://www.debian.org/security/ 2005/dsa-666 Gentoo: http://security.gentoo.org/ glsa/glsa-200502-09.xml Mandrakesoft: http://www.mandrakesoft.com/security/ advisories?name=MDKSA-2005:035 Trustix: http://www.trustix.org/errata/2005/0003/ Red Hat: http://rhn.redhat.com/errata /RHSA-2005-109.html SUSE: ftp://ftp.SUSE.com/pub/SUSE **Debian:** **http://security.debian.org/pool/ updates/main/liba/libapache-mod-python/** Currently we are not aware of any exploits for this vulnerability.	Python SimpleXMLRPCServer Remote Code CAN-2005-0089 CAN-2005-0088	High	Python Security Advisory: PSF-2005-001, February 3, 2005 Gentoo, GLSA 200502-09, February 08, 2005 Mandrakesoft, MDKSA-2005:035, February 10, 2005 Trustix #2005-0003, February 11, 2005 RedHat Security Advisory, RHSA-2005:109-04, February 14, 2005 SUSE Security Summary Report, SUSE-SR:2005:005, February 18, 2005 US-CERT VU#356409 **Debian Security Advisory, DSA 689-1, February 23, 2005**
Raven Software Soldier of Fortune II 1.03 gold and prior	A vulnerability exists that could let a a remote malicious user cause the target game service to crash. A remote user can send a specially crafted cl_guid value to trigger a memory access error. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Raven Soldier of Fortune II Denial of Service Vulnerability CAN-2005-0568	Low	SecurityTracker Alert ID: 1013291, February 24, 2005

Sun Microsystems, Inc. Sun Java JRE 1.3.x, 1.4.x, Sun Java SDK 1.3.x, 1.4.x; Conectiva Linux 10.0; Gentoo Linux; HP HP-UX B.11.23, B.11.22, B.11.11, B.11.00, HP Java SDK/RTE for HP-UX PA-RISC 1.3, HP Java SDK/RTE for HP-UX PA-RISC 1.4; Symantec Gateway Security 5400 Series v2.0.1, v2.0, Enterprise Firewall v8.0	A vulnerability exists due to a design error because untrusted applets for some private and restricted classes used internally can create and transfer objects, which could let a remote malicious user turn off the Java security manager and disable the sandbox restrictions for untrusted applets. Updates available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57591-1 Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-38.xml HP: http://www.hp.com/go/java Symantec: http://securityresponse.symantec.com/avcenter/security/Content/2005.01.04.html SuSE: ftp://ftp.suse.com/pub/suse/ **Apple:** **http://docs.info.apple.com/article.html?artnum=300980** Currently we are not aware of any exploits for this vulnerability.	Sun Java Plug-in Sandbox Security Bypass CAN-2004-1029	Medium	Sun(sm) Alert Notification, 57591, November 22, 2004 US-CERT VU#760344, November 23, 2004 Conectiva Linux Security Announcement, CLA-2004:900, November 26, 2004 Gentoo Linux Security Advisory, GLSA 200411-38, November 29, 2004 HP Security Bulletin, HPSBUX01100, December 1, 2004 Sun(sm) Alert Notification, 57591, January 6, 2005 (Updated) Symantec Security Response, SYM05-001, January 4, 2005 SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 **Apple Security Update, APPLE-SA-2005-02-22, February 22, 2005**
Symantec Firewall/VPN Appliance 200/200R (firmware builds prior to build 1.68 and later than 1.5Z) Gateway Security 360/360R (firmware builds prior to build 858) Gateway Security 460/460R (firmware builds prior to build 858) Nexland Pro800turbo (firmware builds prior to build 1.6X and later than 1.5Z)	Vulnerabilities exist in various Symantec firewall devices, which may disclose sensitive information to malicious people. This is due to an error in the SMTP binding functionality of certain devices with ISP load-balancing capabilities. The vendor has issued updated firmware releases: http://www.symantec.com/techsupp Currently we are not aware of any exploits for these vulnerabilities.	Symantec Firewall Devices SMTP Binding Configuration Bypass	Medium	Symantec Security Bulletin, SYM05-004, February 28, 2005
Trend Micro Client / Server / Messaging Suite for SMB Client / Server Suite for SMB InterScan eManager InterScan Messaging Security Suite InterScan VirusWall InterScan Web Security Suite InterScan WebManager InterScan WebProtect for ISA OfficeScan Corp. Edition PC-cillin Internet Security PortalProtect for SharePoint ScanMail eManager ScanMail ServerProtect	A vulnerability exists in multiple Trend Micro virus products that could let a remote malicious user execute arbitrary code. This is due to a boundary error in the AntiVirus library when processing ARJ files that could be exploited to cause a heap-based buffer overflow. Update information available at: http://www.trendmicro.com/vinfo/secadvisories/default6.asp?VName=Vulnerability+in+VSAPI+ARJ+parsing+could+allow+Remote+Code+execution Currently we are not aware of any exploits for this vulnerability.	Trend Micro AntiVirus Library Heap Overflow CAN-2005-0533	High	Internet Security Systems Protection Advisory February 24, 2005

University of California (BSD License) PostgreSQL 7.x, 8.x	Multiple vulnerabilities exist that could permit malicious users to gain escalated privileges or execute arbitrary code. These vulnerabilities are due to an error in the 'LOAD' option, a missing permissions check, an error in 'contrib/intagg,' and a boundary error in the plpgsql cursor declaration. Update to version 8.0.1, 7.4.7, 7.3.9, or 7.2.7: http://wwwmaster.postgresql.org/download/mirrors-ftp Ubuntu: http://www.ubuntulinux.org/support/documentation/usn/usn-71-1 Debian: http://www.debian.org/security/2005/dsa-668 Gentoo: http://security.gentoo.org/glsa/glsa-200502-08.xml **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/postgresql/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-141.html Gentoo: http://security.gentoo.org/glsa/glsa-200502-19.xml Debian: http://security.debian.org/pool/updates/main/p/postgresql/ Mandrakesoft: http://www.mandrakesoft.com/security/ advisories?name=MDKSA-2005:040 **SUSE: ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for these vulnerabilities.	University of California PostgreSQL Multiple Vulnerabilities CAN-2005-0227 CAN-2005-0246 CAN-2005-0244 CAN-2005-0245 CAN-2005-0247	Medium/ High (High if arbitrary code can be executed)	PostgreSQL Security Release, February 1, 2005 Ubuntu Security Notice USN-71-1 February 01, 2005 Debian Security Advisory DSA-668-1, February 4, 2005 Gentoo GLSA 200502-08, February 7, 2005 Fedora Update Notifications, FEDORA-2005-124 & 125, February 7, 2005 Ubuntu Security Notice,e USN-79-1 , February 10, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0003, February 11, 2005 Gentoo Linux Security Advisory, GLSA 200502-19, February 14, 2005 RedHat Security Advisory, RHSA-2005:141-06, February 14, 2005 Debian Security Advisory, DSA 683-1, February 15, 2005 Mandrakesoft, MDKSA-2005:040, February 17, 2005 SUSE Security Summary Report, SUSE-SR:2005:005, February 18, 2005 **Fedora Update Notifications, FEDORA-2005-157 &158, February 22, 2005** **SUSE Security Summary Report, SUSE-SR:2005:006, February 25, 2005**
Wikimedia Foundation MediaWiki prior to 1.3.11	Multiple vulnerabilities exist in MediaWiki that could let a remote malicious user conduct Cross-Site Scripting attacks and permit a remote authenticated administrator to delete certain files on the system. Input validation errors exist in various fields. A fixed version (1.3.11) is available at: http://sourceforge.net/project/showfiles.php?group_id=34373 Currently we are not aware of any exploits for these vulnerabilities.	Wikimedia MediaWiki Cross-Site Scripting Attacks and Directory Traversal Vulnerability CAN-2005-0534 CAN-2005-0535 CAN-2005-0536	Medium/ High (High if arbitrary code can be executed)	SecurityFocus, Bugtraq ID: 12625, February 28, 2005

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description

March 1, 2005	einstein101.txt	No	Exploit for the Einstein Password Disclosure vulnerability.
March 1, 2005	phpbbsession.c	Yes	Script that exploits the phpBB "autologinid" Security Bypass vulnerability.
March 1, 2005	postnukeSQL0760.txt postnukeXSS.txt postnukeSQL0760-2.txt	Yes	Detailed exploitation for the PostNuke SQL Injection Vulnerability.
February 28, 2005	badBlueExploit.cpp badBlueBufferOverflowExpl.c badblue25.c badblue.cpp	Yes	Exploits for the Working Resources BadBlue MFCISAPICommand Remote Buffer Overflow vulnerability.
February 28, 2005	scrapboom.zip	No	Proof of Concept exploit for the MercurySteam Scrapland Game Server Remote Denial of Service vulnerabilities.
February 26, 2005	ChatAnywhere.c	No	Script that exploits the Chat Anywhere Password Disclosure vulnerability.
February 26, 2005	dbmac.tar.gz	N/A	MacSpoof DB is a database of MAC prefixes for spoofing your MAC address in Linux.
February 26, 2005	eXeem021.c	No	Script that exploits the eXeem Password Disclosure vulnerability.
February 26, 2005	mb111-zk.txt	N/A	MercuryBoard blind bruteforcing utility.
February 26, 2005	phpMyAdmin261.txt	Yes	Detailed exploitation for the phpMyAdmin Cross-Site Scripting and Information Disclosure Vulnerabilities.
February 26, 2005	rkhunter-1.2.1.tar.gz	N/A	Rootkit Hunter scans files and systems for known and unknown rootkits, backdoors, and sniffers.
February 26, 2005	SendLink.c	No	Script that exploits the SendLink Password Disclosure vulnerability.
February 26, 2005	sileAWSxpl_v5.7-6.2.c	Yes	Script that exploits the GNU AWStats Multiple Vulnerabilities.
February 26, 2005	webconnect.pl webconnect.c	Yes	Exploits for the OpenConnect Systems WebConnect Remote Denial of Service and Information Disclosure vulnerability.
February 26, 2005	WifiScanner-0.9.6.tar.gz	N/A	WifiScanner is an analyzer and detector of 802.11b stations and access points that can listen alternatively on all the 14 channels, write packet information in real time, search access points and associated client stations, and can generate a graphic of the architecture using GraphViz.
February 26, 2005	wuftpd262DoS.c	No	Script that exploits the Wu-FTPD Globbing Denial of Service vulnerability.
February 25, 2005	3CDaemon.c	No	Script that exploits the 3Com 3CDaemon Multiple Remote Vulnerabilities.
February 25, 2005	a2ps.c	Yes	Proof of Concept exploit for the GNU a2ps Filenames Shell Commands Execution vulnerability.
February 25, 2005	brute_cisco.exp	N/A	Brute force utility for Cisco password authentication.
February 25, 2005	cfengineRSA.c	Yes	Script that exploits the Cfengine RSA Authentication Heap Corruption vulnerability.
February 25, 2005	cisco-torch-0.3b.tar.bz2	N/A	Cisco Torch mass scanning, fingerprinting, and exploitation tool.
February 25, 2005	exwormshoutcast.c shoutcastPoC.c	Yes	Exploits for the Nullsoft SHOUTcast File Request Format String vulnerability.
February 25, 2005	kNetBufferOverflowPoC.c knetDoS104c.txt	No	Proof of Concept exploit for the Stormy Studios KNet Remote Buffer Overflow vulnerability.
February 25, 2005	PeerFTP_5.c	No	Script that exploits the PeerFTP_5 FTP Password Disclosure vulnerability.
February 25, 2005	savant31FR.txt	No	Exploit for the Savant Web Server Remote Buffer Overflow vulnerability.
February 25, 2005	TCW690.txt	No	Script that exploits the Thomson TCW690 Cable Modem Multiple vulnerabilities.
February 25, 2005	un-typed.c	Yes	Proof of Concept exploit for the Typespeed Format String vulnerability.
February 24, 2005	sof2guidboom.zip	No	Exploit for the Raven Software Soldier Of Fortune 2 Remote Denial Of Service vulnerability
February 23, 2005	elog_unix_win.c	No	Script that exploits the ELOG Web Logbook Attached Filename Remote Buffer Overflow vulnerability.
February 23, 2005	prozillaFormatString.c	No	Script that exploits the ProZilla Initial Server Response Remote Client-Side Format String vulnerability.
February 23, 2005	unAceBufferOverflowPOC.zip	No	Script that exploits the Winace UnAce Buffer Overflow vulnerability.

[back to top]

Trends

- A redirection script on eBay's site is being exploited by phisers that makes fraudulent emails look more convincing. For more information, see "eBay provides backdoor for phishers" located at: http://www.theregister.co.uk/2005/02/28/ebay_phishing_backdoor/.
- Federal authorities are investigating two e-mail scams, including one targeting families of soldiers killed in Iraq, that claim to be connected to the Homeland Security Department. For more information, see: "E-Mail Scams Exploit Homeland Security And Soldiers Killed In Iraq" located at: http://www.informationweek.com/story/showArticle.jhtml?articleID=60402476
- Britain’s Home Office has launched a high-profile campaign to secure the Internet against hacking groups using networks of infected computers to launch worm, spam and denial of service attacks against critical businesses and services. The campaign, which features a Website and an alert service to help non-IT specialists protect their computer systems, is designed to plug one of the weakest links in security on the Internet: home and small business PCs. The campaign will encourage home users and small businesses to sign up to an alert service, run by the National Infrastructure Security Coordination Centre (NISCC), part of the Home Office, which will give advice on urgent threats that affect home PCs, PDAs and mobile phones. . For more on the new service, visit http://www.itsafe.gov.uk. For more information, see "Home Office in drive to stamp out botnets" located at: http://www.computerweekly.com/articles/article.asp?liArticleID=136955&liArticleTypeID=1&liCategoryID=2&liChannelID=22&liFlavourID=1&sSearch=&nPage=1

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Bagle.BJ	Win32 Worm	Increase	January 2005
2	Netsky-P	Win32 Worm	Slight Decrease	March 2004
3	Zafi-D	Win32 Worm	Slight Decrease	December 2004
4	Netsky-Q	Win32 Worm	Stable	March 2004
5	Zafi-B	Win32 Worm	Decrease	June 2004
6	Netsky-D	Win32 Worm	Slight Decrease	March 2004
7	Netsky-B	Win32 Worm	Slight Increase	February 2004
8	Bagle-AU	Win32 Worm	Increase	October 2004
9	Lovegate.W	Win32 Worm	New to Table	April 2004
10	Bagle-BB	Win32 Worm	Return to Table	September 2004

Table Updated March 1, 2005

Viruses or Trojans Considered to be a High Level of Threat

- BagleDl-L: A new variant of Bagle, BagleDl-L, is a Trojan horse that damages security applications and attempts to connect with a number of Web sites. According to antivirus companies F-Secure and Sophos, these Web sites currently contain no malicious code, but both companies believe this could soon change. For this Trojan to work, a certain amount of social engineering is required because the e-mails contain a ZIP-file attachment that must be opened to display the programs "doc_01.exe" or "prs_03.exe," which must also be run manually to infect a computer. For more information see: http://news.com.com/New+Bagle+damages+security+software/2100-7349_3-5594201.html?tag=nefd.top

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Bagle.BD	Email-Worm.Win32.Bagle.bd Email-Worm.Win32.Bagle.pac	Win32 Worm
Bagle.BF	Email-Worm.Bagle.BF	Win32 Worm
Download.Sumina		Trojan
Downloader-VQ		Trojan
Keylog-Sters		Trojan
Mitglieder.BO	Trj/Mitglieder.BO	Trojan
MultiDropper-MI		Trojan
Mytob.A	W32.Mytob@mm W32/Mydoom W32/Mytob.A.worm Win32/Atak.Variant!Worm WORM_MYTOB.A	Win32 Worm
Mytob.B	Net-Worm.Win32.Mytob.a W32.Mytob.B@mm W32/Mydoom.b@mm WORM_MYTOB.B	Win32 Worm
Proxy-Agent.g	Trojan-Proxy.Win32.Small.ba Win32/TrojanProxy.Small.BA	Trojan
PWS-Goldun.dr		Trojan
PWS-QQRob	TR/Dldr.Delf.CQ Trojan-PSW.Win32.QQRob.13 TROJ_DELF.IQ Win32.QQRob.C	Trojan
PWSteal.Ldpinch.D		Trojan
Stang.B	W32/Stang.B.worm	Trojan

Troj/Dloader-IE	Trojan-Downloader.Win32.Delf.ij	Trojan
Troj/Kelebek-G	Backdoor.IRC.Kelebek.g	Trojan
TROJ_BAGLE.A		Trojan
Trojan.Dremn		Trojan
Trojan.Tooso.B		Trojan
Trojan.Tooso.C		Trojan
Trojan.Tooso.D		Trojan
Trojan.Win32.Lazar.a	Lazarus Lazarus.2222 Trojan.Lazar	Trojan
Trojan-Dropper.Win32.Small.tl	Email-Worm.Win32.Bagle.al Small.TL	Trojan
W32.Beagle.BG@mm	W32.Beagle.BH@mm W32/Bagle.bn@MM Win32.Bagle.AZ Win32.Bagle.BA WORM_BAGLE.BE	Win32 Worm
W32.Bobax.N	W32/Bobax.worm Win32.Bobax.R WORM_BOBAX.AA	Win32 Worm
W32.Conycspa.G@mm	QLowZones-4.dldr Trojan-Downloader.Win32.CWS.gen Trojan.Bookmarker	Win32 Worm
W32.Derdero.E@mm		Win32 Worm
W32.Elitper.A@mm		Win32 Worm
W32.Holcas.A@mm	IRC.Generic IRC/Generic* MIRC/Generic mIRC/Simp-Fam mIRC/Worm.Variant!Worm WORM_HOLCAS.A	Win32 Worm
W32.Holcas.A@mm		Win32 Worm
W32.Looked.C	W32/Generic.Delphi.b Worm.Win32.Viking.a	Win32 Worm
W32.Namshare		Win32 Worm
W32.Randex.CST	Backdoor.Win32.SdBot.gen W32/Sdbot.worm.gen.j	Win32 Worm
W32.Refaz		Win32 Worm
W32.Spybot.KAI		Win32 Worm
W32.Spybot.KEG		Win32 Worm
W32.Stang	Stang.A W32/Stang.A.worm	Win32 Worm
W32/Agobot-OV	Backdoor.Win32.Agobot.gen	Win32 Worm
W32/Agobot-QE		Win32 Worm
W32/Agobot-QL	Backdoor.Win32.Agobot.yt	Win32 Worm
W32/Assiral-B		Win32 Worm
W32/Bagle.BG.worm	Bagle.BG Email-Worm.Win32.Bagle.bg Email-Worm.Win32.Bagle.pac	Win32 Worm
W32/Bagle.BL	Email-Worm.Win32.Bagle.bb Troj/BagleDl-L W32/Bagle.dldr Win32.Glieder.N Win32.Glieder.N!ZIP Win32/Glieder.N!Trojan	Win32 Worm
W32/Bagle.bn@MM	Bagle.BN W32/Bagle.BN.worm	Win32 Worm
W32/Bagle.bn@MM	Bagle.BN W32/Bagle.BN.worm	Win32 Worm
W32/Bagle.dll.dr	Trojan.Tooso	Win32 Worm
W32/Bropia-Q	WORM_BROPIA.Q	Win32 Worm
W32/Bropia-R	W32.Bropia.R IM-Worm.Win32.Bropia.	Win32 Worm
W32/Bropia-S	IM-Worm.Win32.Bropia.h W32/Bropia.worm.t	Win32 Worm
W32/Codbot-Gen		Win32 Worm
W32/Domwis-G	Backdoor.Win32.Wisdoor.k	Win32 Worm
W32/Forbot-CW	Backdoor.Win32.Wootbot.gen	Win32 Worm
W32/Kelvir-A	IM-Worm.Win32.Kelvir.a W32/Kelvir.worm.a	Win32 Worm

W32/Mydoom.bg@mm	Mytob.A Net-Worm.Win32.E77.a Net-Worm.Win32.Mytob.a W32.Mytob@mm W32/Mytob.A.worm WORM_MYTOB.A	Win32 Worm
W32/Mydoom.bi@MM		Win32 Worm
W32/MyDoom-BD	Email-Worm.Win32.Mydoom.am W32/Mydoom.bd@MM WORM_MYDOOM.BD	Win32 Worm
W32/MyDoom-BG		Win32 Worm
W32/Mytob-C		Win32 Worm
W32/Poebot-I	Backdoor.Win32.Poebot-I BKDR_POEBOT.B	Win32 Worm
W32/Rbot-UC	Backdoor.Win32.Rbot.ex	Win32 Worm
W32/Sdbot.worm.32768		Win32 Worm
W32/Sdbot-VN		Win32 Worm
W32/Sdranck-A	Trojan-Proxy.Win32.Ranky.bc INFECTED W32/Sdbot.worm.gen	Win32 Worm
W32/Sdranck-B		Win32 Worm
Win32.Bagle.AZ	Win32/Bagle.AZ!Worm	Win32 Worm
Win32.Bagle.BA	Win32/Bagle.BA!Worm	Win32 Worm
Win32.Bagle.BB	Bagle.BB Email-Worm.Win32.Bagle.bb Email-Worm.Win32.Bagle.pac	Win32 Worm
Win32.Bagle.BB	Bagle.BB Email-Worm.Win32.Bagle.bb Email-Worm.Win32.Bagle.pac	Win32 Worm
Win32.Bropia.L	IM-Worm.Win32.VB.g W32/Bropia-M W32/Bropia.worm.m W32/Velkdis.A Win32/Bropia.L!Worm WORM_BROPIA.M	Win32 Worm
Win32.Glieder.O	Email-Worm.Win32.Bagle.bd Troj/BagleDl-L W32/Bagle.BL Win32.Glieder.O!ZIP Win32/Glieder.O!Trojan	Win32 Worm
Win32.Glieder.P	Win32.Glieder.P!ZIP Win32/Glieder.P!Trojan	Win32 Worm
Win32.Glieder.Q	Win32.Glieder.Q!ZIP	Win32 Worm
Win32.Toxbot		Win32 Worm
WORM_AHKER.F		Win32 Worm
WORM_BAGLE.BE	Bagle.BE Email-Worm.Bagle.BE TROJ_BAGLE.BE	Win32 Worm
WORM_ELITPER.A		Win32 Worm
WORM_KIPIS.O	Email-Worm.Win32.Kipis.o W32.Kipis.M@mm W32/Kipis W32/Kipis.j@MM	Win32 Worm

[back to top]

Last updated March 02, 2005